State of Wisconsin

CVISN Top-Level Design

Final Version

November 16, 2001

Table of Contents

Introduction

This document is intended to provide general information about Wisconsin's Commercial Vehicle Information Systems and Networks (CVISN) program and specific information about Wisconsin's CVISN Top-Level Design.

CVISN Overview

According to a March 2001 newsletter from the National Conference of State Legislatures, each year trucks and commercial motor carriers travel more than 152 billion miles on America's roads. As demands on the nation's highways and the need for more efficient movement of goods increase, the trucking industry and federal, state and local governments are using Intelligent Transportation System (ITS) technologies to streamline commercial vehicle operations, reduce congestion and improve travel.

The 1998 Transportation Equity Act for the 21st Century (TEA-21) established the goal of deploying CVISN in the majority of the states by 2003. The Federal Motor Carrier Safety Administration (FMCSA) hopes to have CVISN deployed in between 22 and 35 states by 2005. CVISN's goal is to establish a nationwide infrastructure for data exchange for commercial vehicles that are traveling in interstate commerce.

CVISN Defined

The term CVISN refers to the collection of information systems and communications networks that support commercial vehicle operations (CVO). These include information systems owned and operated by governments, motor carriers, and other stakeholders.

The FMCSA-led CVISN program is a public/private effort to establish electronic linkages allowing exchange of motor carrier information between CVO agencies, regional clearinghouses, and national databases. Additionally, the program will establish the communications and computer infrastructure to enable electronic transactions and information exchange between motor carriers and the CVO agencies.

CVISN features electronic fee and tax payments, credential transmittals and recaps, on-line registration and validation, interstate automated information exchange - a plethora of clearance, credentialing, and safety information that will reduce the current costs of state regulatory activities, improve motor carrier compliance, and enhance roadway safety.

CVISN Deployment Levels

The FMCSA is using CVISN "levels" to allow definition of a specific set of capabilities that can be deployed incrementally by a state and its motor carriers. CVISN Level 1 is currently defined, while a definition for CVISN Level 2 is still under discussion.

The following table documents CVISN Level 1 capabilities:

Capability Area	State CVISN Level 1 Capabilities
Safety Information Exchange	▪ ASPEN (or equivalent) at all major inspection sites. ▪ Connection to the Safety and Fitness Electronic Records (SAFER) system to provide exchange of interstate carrier and vehicle snapshots among states. ▪ Implementation of the Commercial Vehicle Information Exchange Window (CVIEW) (or equivalent) system for exchange of intrastate and interstate snapshots within state and connection to SAFER for exchange of interstate snapshots.
Credentials Administration	▪ Automated processing (i.e., carrier application, state application processing, credential issuance, and tax filing) of at least International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) credentials; ready to extend to other credentials [intrastate, titling, oversize/overweight (OS/OW), carrier registration, and hazardous material (HAZMAT)]. Note: processing does not necessarily include e-payment. ▪ Connection to IRP and IFTA Clearinghouses. ▪ At least 10 percent of the transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.
Electronic Screening	▪ Implemented at a minimum of one fixed or mobile inspection site. ▪ Ready to replicate at other sites.

Deployment Process

The recommended state deployment strategy for CVISN Level 1 consists of three key steps: Planning, Design, and Implementation and Deployment.

- **Planning** – This step includes participation in two ITS/CVO training courses and the development of an ITS/CVO State Business Plan. These elements promote ITS/CVO awareness and are essential to effective coalition building among the state agencies involved in CVO and with industry.
- **Design** – The purpose of this step is to permit the state to establish its CVISN project team, including at a minimum a CVISN project manager and a system architect. Once these individuals have been selected, a state can participate in the "Understanding ITS/CVO Technology" training course and in three CVISN Deployment Workshops. These activities will assist the state in developing its CVISN Project Plan and Top-Level Design.
- **Implementation and Deployment** – In the final step (actually a series of steps or phases), states buy or build subsystems and integrate them into their operations to achieve deployment of CVISN Level 1 capabilities.

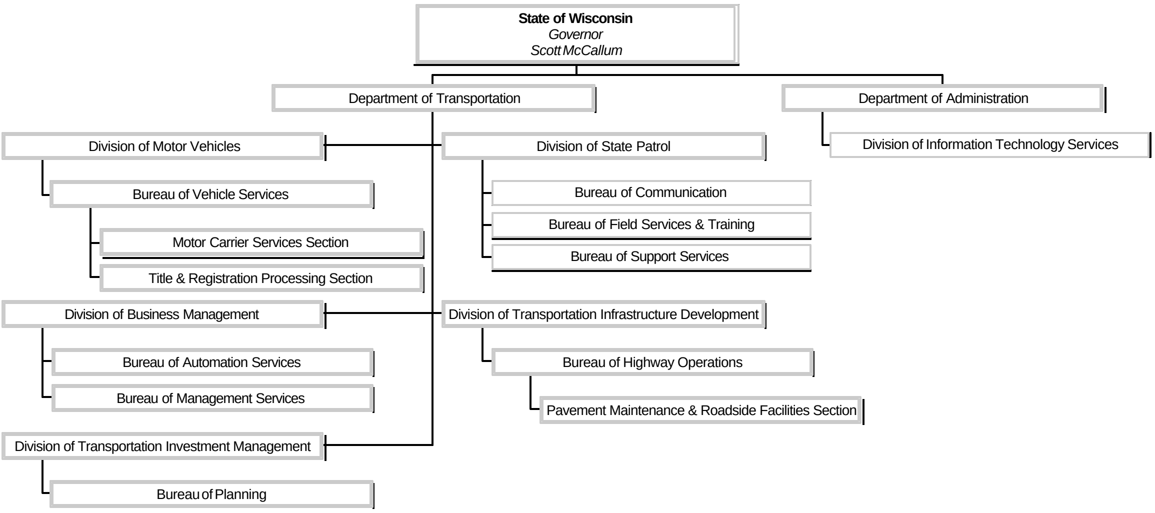
Wisconsin completed its ITS/CVO State Business Plan in 1998 and attended the first two ITS/CVO training courses in 1999. That same year, the Wisconsin Department of Transportation (WisDOT) signed a Memorandum of Agreement and a Partnership Agreement with the United States Department of Transportation (USDOT) to work toward deployment of CVISN Level 1 capabilities. These activities completed the planning step of the deployment process.

In 2000, the CVISN team was established and the third ITS/CVO training course was conducted. The series of three CVISN Deployment Workshops was begun, with participation in the Scope Workshop in October of 2000 and the Planning Workshop in February of 2001. The final CVISN workshop will be held in late May of 2001, where the contents of this document will be presented. Following this workshop, the final CVISN Project Plan and Top-Level Design will be prepared and submitted for approvals. These actions will complete the design step of the deployment process.

The final step of the deployment process, implementation and deployment, will follow approval of the CVISN Project Plan and Top-Level Design. Following the plan, Wisconsin will build or buy various subsystems and integrate them into their existing operations capabilities. Completion of the plan will be dependent upon funding and resource constraints.

Project Organization

Wisconsin is fortunate to have most of the agencies responsible for various aspects of CVISN located in the Department of Transportation. This chart will provide an overview of how the CVISN Program Team is organized.


State of Wisconsin
Governor
Scott McCallum
Department of Transportation
Department of Administration
Division of Information Technology Services
Division of Motor Vehicles
Bureau of Vehicle Services
Motor Carrier Services Section
Title & Registration Processing Section
Division of State Patrol
Bureau of Communication
Bureau of Field Services & Training
Bureau of Support Services
Division of Business Management
Bureau of Automation Services
Bureau of Management Services
Division of Transportation Infrastructure Development
Bureau of Highway Operations
Pavement Maintenance & Roadside Facilities Section
Division of Transportation Investment Management
Bureau of Planning

Primary responsibility for the day-to-day activities of the CVISN project rests with the Steering Committee and the Core Team.

Steering Committee

The Steering Committee is responsible for communicating WisDOT business objectives, setting scope and direction for the project, resolving project issues, determining expected return on investment, providing organizational support, and approving project budget and changes. Members include the Project Sponsors, other key members of WisDOT Executive Management, the Department of Motor Vehicles (DMV) Business Project Manager, the CVISN Project Manager, the CVISN Project Facilitator/Administrator, key WisDOT stakeholders, a representative from the Motor Carrier Industry, and a representative from the Federal Motor Carrier Safety Administration.

Core Team

The Core Team helps drive the project in appropriate directions and assists with issue resolution. Core Team members assist with the preparation of pre-work materials required for USDOT sponsored workshops. They also attend these workshops and assist the CVISN Project Manager with the preparation of the CVISN Project Plan and Top-Level Design. The Core Team meets regularly, advising the CVISN Project Manager when issues and concerns arise and reviewing work in process with an eye toward keeping the CVISN Project focused and functional. Members include the DMV Business Project Manager, the CVISN Project Manager, the CVISN System Architect, the CVISN Project Facilitator/Administrator, and key WisDOT stakeholders from DMV Motor Carrier Services, State Patrol, Bureau of Automation Services, and Division of Transportation Infrastructure Development and representatives from the Federal Motor Carrier Safety Administration and the Federal Highway Administration.

Other ITS Relationships

Several members of the CVISN Core Team also participate in other ITS-related committees within Wisconsin. Examples include the Southwest Wisconsin ITS Architecture Committee, the I-90/94 Corridor Committee, and the Statewide Advanced Traveler Information System Architecture Committee.

Barry Larson, the CVISN System Architect, is chairing the Communications Workgroup for the Southwest Wisconsin ITS Architecture Committee. This group is charged with designing the underlying communication infrastructure for all ITS-related activities within the region and extending statewide.

In collaboration with members of the Bureau of Automation Services ITS group, several members of the Core Team will be mapping our CVISN architecture into the National ITS Architecture using the TurboArchitecture software tool.

Top-Level Design Overview

The top-level design process encompasses setting the scope of the CVISN program in the state, defining top-level requirements, allocating new requirements to new or existing systems, defining interfaces among systems, and describing the physical computers and networks that will support the systems. The top-level design process also focuses on how to use or change the existing systems to support the CVISN operational concepts and scenarios.

The top-level design process results in the definition of:

- User requirements,
- System requirements,
- Allocation of requirements to major system elements, and
- High-level interface specification.

This document provides, in words and pictures, descriptions of each of these areas.

System Requirements

State Specific Goals

Wisconsin intends to satisfy the following objectives via the deployment of CVISN Level 1 capabilities:

- Provide efficient application, processing and delivery of motor carrier credentials (e.g. registration, tax payments, permits, etc.)
- Increase the efficiency and effectiveness of CVO enforcement.
- Enhance safety of commercial vehicle operations.

COACH Part 1 Tables

A state's level of commitment to numerous organizational and technical requirements of the CVISN program is assessed by the completion of several CVISN Operational and Architectural Compatibility Handbook (COACH) documents. Each COACH document is related to a particular category of requirements.

Part 1 of the COACH includes several types of checklists related to operational concepts and top-level design.

- **Guiding Principles** are high-level strategic guidelines.
- **State Institutional Framework Checklists** detail compatibility requirements for the policies and coordinating activities for states.
- **CVISN Operational Concepts and Top-level Design Checklists** document compatibility requirements for processes and top-level compatibility requirements for state designs.

The COACH Part 1 checklists are used to indicate the scope and depth of CVISN Level 1 commitment, and to provide a mechanism for planning development and test activities.

Wisconsin has a full or partial commitment level to each item of the individual checklists with only the few exceptions noted here. The full COACH Part 1 may be found as Appendix A to this document. Wisconsin's no commitment responses include:

Compatibility Criteria	Comments
Jurisdictions will support quarterly reviews of carrier qualifications to ensure that the standards evolve to meet the changing needs of government and motor carriers.	This could take a substantial amount of resources. Who will do quarterly reviews – who rules on the "evolving standards"? We have several different interpretations of this, and are not comfortable with any of them. CVISN is on going – why quarterly reviews? Quarterly reviews are not realistic just to see if a carrier is keeping up-to-date. Evolving standards is a whole different issue.

Compatibility Criteria	Comments
The State has contacted or has plans to contact State and local transportation officials to explore potential joint-uses of transponders and ensure integration among multiple applications (i.e., CVO, toll, traffic probes, parking management, etc.)	We have no input into toll road, fleet and asset management, parking, etc.
Appropriate and sufficient staff, equipment, and State and private funding are available to carry out the deployment of CVISN and ITS/CVO services. The CVISN project has sufficient priority (i.e., other higher-priority projects are not competing for the same resources).	Funding and resource availability are critical issues for Wisconsin's ability to achieve CVISN Level 1 capabilities by the Federal target date of September 30, 2003.
Electronic access to administrative processes and information is available from "one stop shops" in public sites.	Means PCs at counters. Either from the carrier or carrier agents.

Other State Requirements

Wisconsin has decided to include the Oversize Overweight Permit Processing System (OOPPS) as part of our overall CVISN effort. This system has been in development for over a year, and certain capabilities are currently in production. Other functions are being added using a phased approach.

To ensure interoperability between these OSOW applications and other CVISN-related applications, we are being on the alert for areas where standardization is required.

System Design

Allocation of Requirements to System Components

COACH Part 3 Tables

COACH Part 3 is meant to document how Wisconsin might allocate various requirements detailed in the COACH Part 1 to elements of our system design.

Wisconsin has a full or partial commitment level to each item of the individual checklists with only the few exceptions noted here. The full COACH Part 3 may be found as Appendix C to this document. Wisconsin's no commitment and significant partial commitment responses include:

Compatibility Criteria	Comments
Use of ISS-2 algorithm	No commitment at this time, but possible future implementation.
Treasury System	Our partial commitment response refers to the acceptance of electronic payments. The definition of CVISN Level 1 specifically excludes the ability to accept electronic payments. However, Wisconsin is currently conducting a pilot project that, when approved, will allow all state agencies to accept credit cards for payment. It is questionable whether our DMV Revenue system would have this functionality added.
HazMat	Wisconsin does not have a HazMat system in place.
Various uses of ANSI X12 EDI	Various no commitment and partial commitment responses were primarily related to one of two overall themes. ▪ Some of our systems use AFF or other data exchange methods. We made an early design decision to not alter connections that already exist in our legacy systems. ▪ Our support for other uses of EDI is pending a viable alternative such as XML for exchanging data.

COACH Part 4 Tables

The COACH Part 4 checklists are used to indicate the level of commitment to various interfaces between internal and external CVISN systems.

It is Wisconsin's intention to incorporate the CVISN Level 1 Interface Standards in the state's CVISN design and deployment plans. The following will summarize the general approach reflected in the design and deployment plans.

Interface Design Overview

The Wisconsin design adheres to the ANSI X12 EDI standards for system-to-system communication between carrier and state. It also will employ appropriate Internet standards for carrier-to-state communications involving carrier browser connections to the state web site(s). Although we are committed to EDI as the method for system-to-system communication, it is our preference to use XML at some future date. Our initial deployment will be directed to carrier browser connections to the web site(s). Should standards become available for an XML carrier to state data exchange alternative prior to Wisconsin beginning development of an EDI based system-to-system capability, we will skip the EDI deployment and move directly to an XML approach.

Communication among state Commercial Vehicle Administrative systems will employ Application File Format (AFF). The goal is to minimize changes to existing legacy applications by continuing to use the communications syntax native to those applications. The exception to this regards communication with the IRP and IFTA systems. Wisconsin utilizes The Polk Company's COVERS and COVERSft products and has specified that the communication with these applications be done using the CVISN prescribed X12 EDI Transaction Sets. The intention is to isolate the state from vendor system formats to the extent possible, such that a product change sometime in the future would have its impact reduced to some degree.

Communication between state Commercial Vehicle Administrative Systems and the Roadside systems will also use AFF, again to minimize the changes necessary to be made on the existing legacy applications. Roadside systems only communicate with state systems and have will have no direct connections with Core Infrastructure Systems. Roadside System communication with Carrier Commercial Vehicles will employ CVISN Level 1 standards as outlined in COACH Part 4.

Wisconsin will adhere to the CVISN Level 1 standards between state Commercial Vehicle Administrative Systems and Core Infrastructure Systems as described in COACH Part 4. Although we are intending to employ EDI at the outset, the XML alternative is our preferred approach. Toward that end, our initial CVIEW development will isolate the CVIEW/SAFER EDI data exchange functionality as much as possible in anticipation of moving to the XML data exchange alternative. We are participating in the SAFER Options Working Group (SOWG) and will continue to do so. The recent APL document "SAFER Option Working Group Schedules and Deliverables", dated April 24th, 2001, is of great interest to us. If the proposed schedule is adopted, the Wisconsin CVIEW development (Build 2) would likely target the XML exchange alternative rather than EDI, since the proposed schedule is an excellent fit with Wisconsin's anticipated development and deployment plans.

COACH Part 4 – Table 2-1 Exceptions

The following are exceptions from full commitment to the items in Table 2-1. The Interface Design Overview of the previous page was intended to provide a context for these exceptions. Wisconsin's no commitment items include:

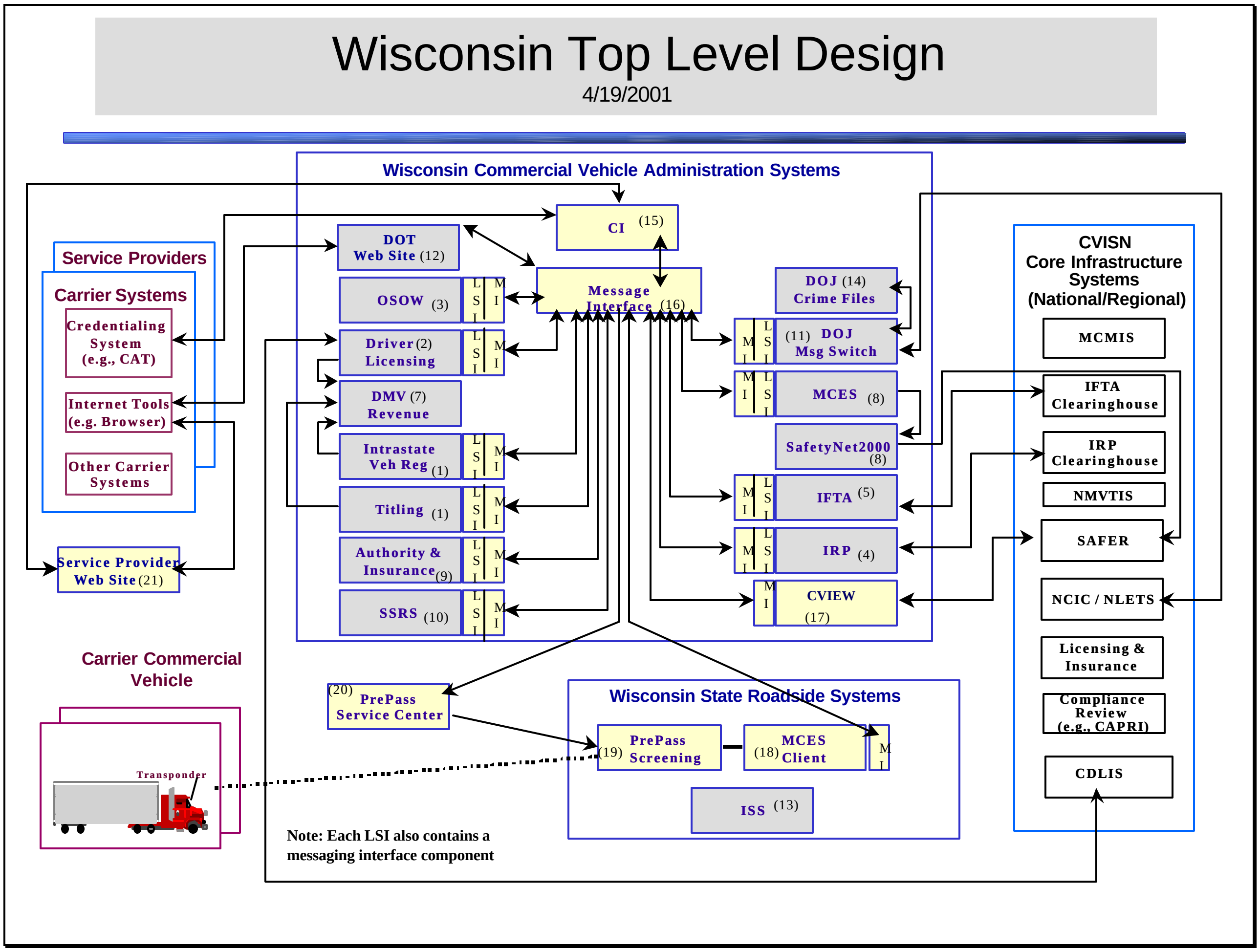
Compatibility Criteria	Comments
EDI-C	Communication among state systems will employ AFF with the exception of vendor-supplied systems such as IRP and IFTA.
EDI-F	Communication between state administrative and roadside systems will use AFF.
EDI-N	Aspen equivalent is used. Communication between state administrative and roadside systems will use AFF.
EDI-X	Law enforcement communication with SAFER is via the CVIEW. No direct connection.
AFF-A	No ASPEN equivalent direct connection to SAFER. We will use CVIEW as the link to SAFER.
AFF-B	No ASPEN equivalent direct connection to SAFER. We will use CVIEW as the link to SAFER.
AFF-E	ASPEN equivalent uploads directly to SAFETYNET 2000. Does not employ SDM to populate SAFETYNET 2000.
AFF-H	ASPEN equivalent uploads directly to SAFETYNET 2000. Does not employ SDM to populate SAFETYNET 2000.
CIA-C	No direct connection from ASPEN (equivalent) to SAFER. CVIEW is the link to SAFER.
CIA-D	No direct connection from ASPEN (equivalent) to SAFER. CVIEW is the link to SAFER.
CIA-E	ASPEN equivalent uploads directly to SAFETYNET 2000. Does not employ SDM to populate SAFETYNET 2000.
CIA-F	ASPEN equivalent uploads directly to SAFETYNET 2000. Does not employ SDM to populate SAFETYNET 2000.

Top Level Design

The Top Level Design incorporates the following underlying design principles:

- Application system integration required by CVISN will be accomplished using a messaging / queuing approach.
- Communication among internal state systems will continue to use syntax native to those systems to minimize legacy system changes.
- State application system interfaces to external systems will be minimized to the greatest extent possible.
- Updates from state credentialing and safety systems will be applied on a real time transactional basis to a state summary database (CVIEW), which in turn forwards updates to SAFER.

Wisconsin's Top Level Design reflects a concerted effort to tie existing legacy systems and newly acquired applications together in a manner that can respond to future changes.



1) The DMV Registration System that runs in the FileHandler environment (file 10) is the single system that maintains registration, title and VIN information for all vehicle types. The Titling, and Intrastate Registration requirements are both addressed by this single system. This system runs on an OS/390 mainframe operated by the Wisconsin Department of Administration (DOA). A Legacy System Interface / Messaging Interface (LSI / MI) will be added.
2) The DMV Drivers System that runs in the CICS/DB2 environment is the single system that maintains current and driver history information for all Wisconsin drivers license classification types. There is also a mirror image of this database running in the FileHandler (file 60) environment. Transactions simultaneously update both databases. The FileHandler based Drivers database will be eliminated when all drivers related processing functions are fully migrated to the new CICS/DB2 environment. Both of these systems run on an OS/390 mainframe system operated by the DOA. A LSI / MI will be added.
3) The OSOW application runs in a Visual Basic / DB2 environment. This application also has a web interface for application submittal used by a limited number of carriers at this time. The database server component of the system runs on an OS/390 mainframe operated by the DOA. The Application server runs on a DOT NT machine. A LSI / MI will be added.
4) The IRP system is the Polk COVERS application. The database is Oracle, running on the DOT HP 9000N Oracle Server. The COVERS application runs on roughly 30 workstations attached to a DMV LAN. Users external to the DMV Motor Carrier workgroup DO NOT have connectivity to the IRP database. This information is provided to the Motor Carrier inspectors by a nightly batch run which gathers the updates applied to the Oracle database and creates a set of update transactions to apply to the Motor Carrier Enforcement System (MCES) that all permanent scale locations have online access to. It also updates (file 56) the IRP Registration file running under FileHandler. A LSI / MI will be added.
5) The IFTA system is the Polk COVERSft application. The database is Oracle, running on the DOT HP 9000N Oracle Server. The IFTA and IRP information have been combined in a single Oracle database. The COVERSft application runs on roughly 30 workstations attached to a DOT LAN. Users external to the DMV Motor Carrier workgroup DO NOT have connectivity to the IFTA database. The COVERSft application handles both IFTA Registration & IFTA tax processing. A LSI / MI will be added.
6) The Wisconsin Department of Natural Resources (DNR) maintains a paper file of proof of insurance for Hazardous Waste transporters. This is $300,000 coverage per fleet. DNR issues WDNR #'s indicating coverage is on file. DNR's responsibility is for Haz waste, not Haz materials. There are no automated systems involved.
7) DMV Revenue is the DMV revenue accounting system operated by the Revenue Accounting Unit located in the DMV Bureau of Driver Services. The system is a combination of FileHandler and CICS/DB2 applications. Roughly 90% of the applications are CICS/DB2. Outputs from this system are journal entries for the FOS system, the DOT departmental accounting system. This system runs on an OS/390 mainframe operated by the DOA.

8) The Motor Carrier Enforcement System (MCES) is a CICS/DB2 system that runs on an OS/390 mainframe operated by the DOA. All fixed scale locations have access to the system via T1 leased line connections employing IP protocol. One function provided by the MCES is to automate the inspection report creation process. It has the ability to make plate, driver and carrier queries to populate the fields for Wisconsin based vehicles for example. Inspection reports are printed at the fixed scale location, and a record of the inspection report is maintained in the MCES DB2 database.

   A second function of the system is to provide the inspector with background information on the carrier, driver, and vehicle. This information is available for carriers, vehicles, and drivers which State Patrol inspectors have had a contact with in the past, either interstate or intrastate. Information includes: inspection report, size/weight, incidents, and crash supplements.

   A weekly batch job is run to extract the new inspection reports from MCES, and automatically load the required information into SAFETYNET. SAFETYNET in turn periodically uploads the info to MCMIS. SAFETYNET will be replaced with SAFETYNET2000, in which case its core system connection will be with SAFER and not MCMIS. MCES will continue to be the data source.

   The mobile inspectors currently have mobile data computers (MDC). MDC software will be upgraded with IP protocol capability to enable access to MCES via the DOJ message switch. A LSI / MI will be added to MCES.

9) Carrier Authority and Insurance System that runs in the FileHandler environment (file 17) maintains carrier authority and insurance status for intrastate carriers and interstate carriers base stated in Wisconsin. The system runs on an OS/390 mainframe operated by the DOA. A LSI / MI will be added.

10) The Single State Registration System (SSRS) addresses the requirement that interstate carriers register their USDOT operating authority with their base state. Wisconsin registers interstate for-hire carriers, collects permit fees for Wisconsin and other states, and transmits other state’s fees on a monthly basis. This system runs in the FileHandler environment and runs on an OS/390 operated by the DOA. A LSI / MI will be added.

11) The DOJ Message Switch is a store and forward Unix machine operated by the Wisconsin Dept of Justice. The machine serves as the hub in linking together most Wisconsin law enforcement agencies ranging from local law enforcement, the State Patrol, and agencies such as DOT and DOJ that are data providers for the law enforcement community. The switch also has T1 leased-line connectivity to NCIC and NLETS enabling Wisconsin law enforcement connection with other states and NCIC information. Most law enforcement organizations have T1 connections to the switch. A LSI / MI will be added.

12) The DOT web site provides Web enabled carrier access to motor carrier credentialing services. It is anticipated that the existing OSOW Web Site would be enhanced to provide Web access to IRP and IFTA as well.

13) The ISS system provides motor carrier safety profiles and is an important tool in the motor carrier inspector's current screening process. The ISS system runs on laptop computers and has no connectivity to other systems. The ISS application on the laptop is updated quarterly with a CD received from FMCSA. (Manual process)

14) DOJ crime files contain wants & warrants and stolen vehicle info for Wisconsin. This is similar to NCIC but only statewide in scope.

15) The Credential Interface (CI) is a new component to be added. It will be the sole state interface point for EDI transactions from carriers and carrier agents. Its principal function is to receive transactions from carriers or agents, send acknowledgements and products back to the carrier or agent, and to provide basic editing for application completeness. It will also provide EDI (eventually XML) translations to and from internal state system formats. Communication among state legacy systems will continue to use the syntax native to the legacy systems. EDI will be used for external interfaces & vendor supplied products such as IRP & IFTA.

16) The Messaging Interface (MI) is a new component to be added. It is closely integrated with the CI and provides messaging and queuing services. Conceptually, the MI would have scripts associated with specific application transaction types that would enable it to:

    - Receive and store transactions arriving from carriers and agents.
    - Spawn transactions to other systems to gather status information needed by a credentialing or safety system to process an incoming transaction.
    - Assemble "Information Packages" (the incoming carrier application transaction, and required status information) and forward to appropriate credentialing system.
    - Translate between various Application File Format (AFF) data structures used by legacy systems.
    - Route acknowledgements and credentialing system products to CI for distribution to carriers or agents.
    - Route credentialing and safety system updated status to CVIEW.
    - Return detailed credential information in response to an enforcement query from the MCES client.
    - Route Snapshots from CVIEW to roadside systems.
    - Route Snapshots to the PrePass Service Center (periodically)

    The MI will be constructed using IBM's MQSeries middleware software. Middleware is the software "glue" that helps distributed applications and databases work together. A brief explanation follows, with more complete information available in Appendix F.

    Message queuing is a method of program-to-program communication. Programs within an application communicate by writing and retrieving application-specific data (messages) to and from queues without having a private, dedicated, logical connection to link them.

Messaging means that programs communicate with each other by sending data in messages and not by calling each other directly. Queuing means that programs communicate through sequential transaction lists known as queues. Programs communicating through queues need not be executed concurrently.

Since MQSeries communicates via queues it can be referred to as using indirect program-to-program communication. The programmer cannot specify the name of the target application to which a message is sent. However, he or she can specify a target queue name; and each queue is associated with a program. An application can have one or more "input" queues and may have several "output" queues containing information for other servers to be processed, or for responses for the client that initiated the transaction.

17) The CVIEW is a new component to be added. The CVIEW will be the interface point between state systems and the Federal SAFER system. State credentialing and safety systems will provide status updates to CVIEW via the Messaging Interface. The CVIEW will be the states snapshot repository for intrastate carrier and vehicle information as well as for selected subsets of SAFER interstate carrier and vehicle information.

    Note: Although the design presumes the use of the EDI/post office protocol as the data exchange mechanism with SAFER, it is anticipated an FTP/XML or flat file data exchange alternative will become available. CVIEW detail design will isolate the data exchange facility to the extent possible to minimize rework, in the event the FTP/XML alternative isn't available at the time of Wisconsin's CVIEW development.

18) The MCES Client is a new component to be developed and provides the functions associated with the Roadside Operations Computer (ROC), i.e. interface to CVIEW to get snapshot data, and to provide roadside access to state source systems. It also, in conjunction with MCES, provides the ASPEN equivalent automated inspection reporting function.

19) The PrePass Screening Computer is a new component to be added. This is supplied as part of the PrePass program. The Screening Computer is used to make the screening decision (pull in or by pass) based on sensor inputs and the snapshot screening criteria. We expect the MCES Client will ultimately connect to the PrePass Screening Computer to obtain the VIN #'s for vehicles receiving a pull in signal. The MCES Client will use these VIN #'s to query state source systems for detail information to be made available to the roadside inspector, without needing to manually key the inquiries.

20) The state CVIEW snapshot information will be periodically supplied to the PrePass service center CVIEW equivalent. An Internet IP connection will be employed as the transport mechanism.

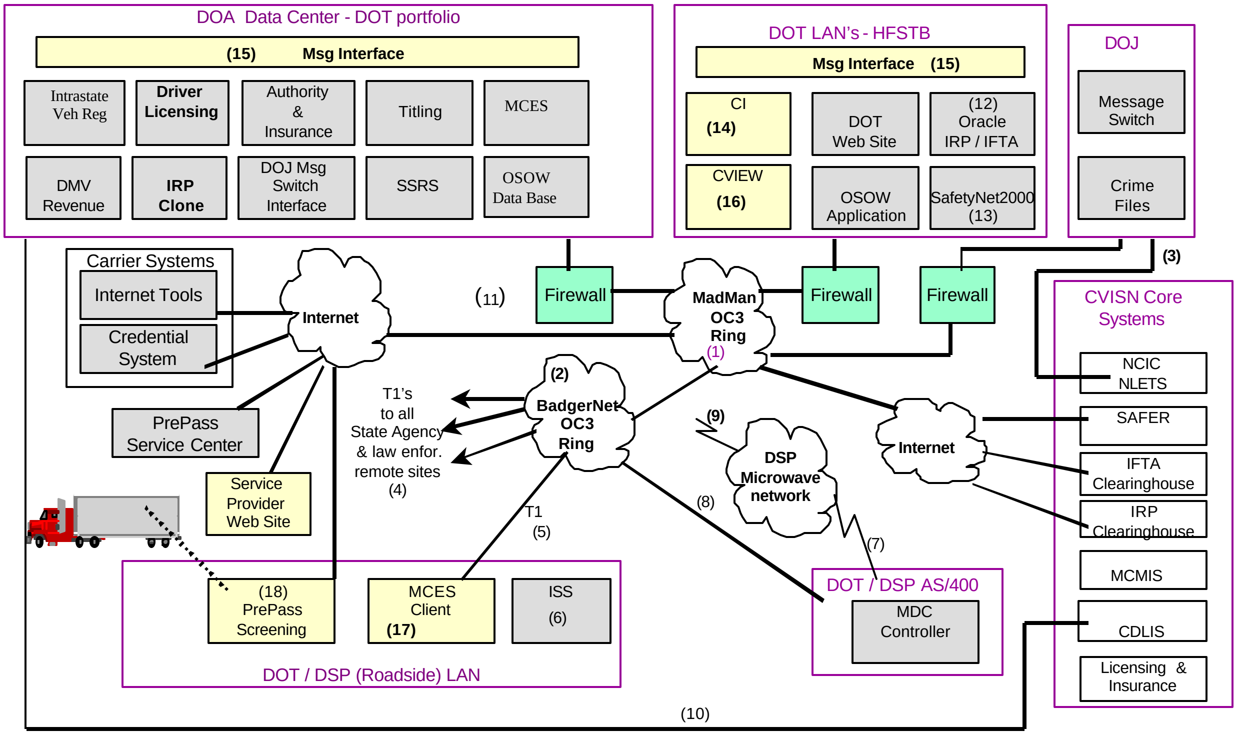
21) The service provider web site is another option for carriers to use for submitting electronic credentialing applications to the state. The Polk COVERSnet product is an example of this type of service. It in turn routes the completed application to the state CI/MI.

Top-Level Physical System Design

Wisconsin's top-level physical design reflects the significant investments the State has made in its computing and network infrastructure. Because of this planning and investment, Wisconsin will require minimal additional investment to support CVISN Level 1 deployment efforts.

Wisconsin Top Level Physical Design

4/19/2001



1) MadMan is a high-speed network connecting all major agency headquarters locations in the Madison Metro area. Although it has the appearance of an OC3 ring, it is implemented as a fully meshed network of LightStream 1010 ATM switches. There are three LS1010's, one located at the DOT, one at the Department of Administration (DOA), and one at the Department of Workforce Development (DWD). Each Switch has two OC3 paths to the other two switches, thus the appearance of a true ring. Each large agency has two head end routers at their headquarters location, which are in turn connected to two of the MadMan LS1010's. The head end routers are Cisco's with ATM cards, and generally are of the 7200 or 7500 series. Twelve agencies, the legislature, Governors Office and the Supreme Court have connectivity to MadMan. MadMan is connected via two OC3 links to BadgerNet, the statewide ATM network. MadMan thus provides agency connections to their remote locations, to other state government agencies and governmental branches, and to the Internet.

   WiscNet is a non-profit organization of the University of Wisconsin and serves as the Internet Service Provider of choice for state agencies, and most Wisconsin school districts. Two OC3 connections are provided between MadMan and WiscNet, which is located on the UW Madison campus. WiscNet in turn has redundant paths to the Internet, one an OC3 connection from the UW Madison campus to Chicago NAPNET, and a second OC3 path from the UW Milwaukee campus to Chicago NAPNET.

2) The BadgerNet is Wisconsin's statewide data and full motion video network. The backbone is an OC3 SONET ring, with 19 ATM switch nodes located throughout the state. The ATM switches are Cisco Stratacoms, and are located at most University of Wisconsin campuses, as well as a number of Wisconsin Tech College locations. The switches are equipped with MGX access shelves that provide link layer conversion from ATM to Frame Relay and vice versa. The BadgerNet SONET backbone and MadMan are running ATM, the access links from remote site routers to the MGX side of the nearest ATM switch are running frame relay.

   BadgerNet currently has approximately 1800 end points that include nearly all of the state agency remote locations, all school districts, and most law enforcement agencies.

   Minimum access bandwidth is T1, with a number of locations having DS3 access links.

3) The DOJ Message switch connection to NCIC & NLETS is a T1 leased line running TCP/IP. Both NCIC & NLETS traffic are carried on the same link.

4) BadgerNet provides the router and managed router service for all state agency connections. Connection speeds are T1 minimum. Connections provided for school districts are terminated at the CSU/DSU. The router and router management is provided by the ISP for this customer base.

5) The MCES client connections at fixed SWEF locations are currently 56kb SNA leased line connections. The 3174 cluster controllers will be replaced with LAN's at each location, and the current low speed network connections replaced with BadgerNet T1 access. This will run TCP/IP protocol, as do all BadgerNet access connections.
6) The ISS system is loaded on laptop computers at both fixed and mobile inspection facilities, and has no network connectivity. ISS applications on laptops are updated quarterly with CD's received from FMCSA.
7) The AS/400 and 6 attached gateways serve as the Mobile Data Computer (MDC) network controller. The Division of State Patrol (DSP) microwave system functions as the wireless backbone network, providing MDC access statewide. All DSP squad cars and motor carrier mobile inspection vehicles have MDCs installed. Approximately 90 local law enforcement agencies also have MDCs in their squads. They also use the DSP backbone. They currently have access to DMV Driver and Registration databases as well as inquiry capability into DOJ Crime Files and NCIC. MDCs don't currently have access to MCES. The MDC system employs a proprietary protocol, and transmission speeds are limited to roughly 4.8KB. An effort has been underway with the MDC vendor to upgrade the software to provide an IP protocol stack, but a functional product isn't expected until mid 2001 at the earliest. MCES access will then be available for MDCs, as well as access to other state source systems. Cellular communication is currently being piloted as an alternative and offers the same functionality as at the SWEF.
8) The connection from the AS/400 to the DMV & DOJ systems is a standard T1 BadgerNet link, employing TCP/IP.
9) Microwave connection to vehicles having MDC equipment installed.
10) The connection from the DOA data center to CDLIS and other states are two 19.2KB AAMVANET leased lines running SNA protocol. These are in the process of being replaced with a 256kb frame relay line. The CDLIS traffic will be carried as encapsulated SNA until such time as the CDLIS application is upgraded to IP.
11) The firewall configuration is depicted in a separate diagram.
12) A dial up connection is currently employed between the Polk COVERSft (IFTA) application and the IFTA Clearinghouse. This will be replaced with an Internet IP connection.
13) A dial up connection was used to upload the SafetyNet data to MCMIS. This will be replaced with SAFETYNET 2000 to SAFER employing an Internet IP connection.

14) The CI will be the sole state interface point for EDI transactions from carriers and carrier agents. Its principal function is to receive transactions from the carriers or agents, send acknowledgements and products back to the carrier or agent, and to provide basic editing for application completeness. It will also provide EDI (eventually XML) translations to and from internal state system formats. Communication among legacy systems internal to the state will continue to use the syntax native to the legacy system. The exception is for vendor-supplied applications such as IRP and IFTA that will use EDI, as well as external interfaces to carrier systems and federal systems.

15) The Messaging Interface is closely integrated with the CI and provides messaging and queuing services. Conceptually, the Messaging Interface would have scripts associated with specific application transaction types that would enable it to:

    a) Receive and store transactions arriving from carriers and carrier agents.
    b) Spawn transactions to other systems to gather status information needed by a credentialing system to process an incoming transaction.
    c) Assemble "information packages" (the incoming carrier application transaction, and required status information) and forward to appropriate credentialing system.
    d) Send acknowledgements and credentialing system products back to carrier or carrier agent.
    e) Route credentialing system updated status to CVIEW.
    f) Return detailed credential information in response to an enforcement query from the MCES client.
    g) Route Snapshots from CVIEW to roadside systems.
    h) Route selected Snapshots to PrePass Service Center CVIEW equivalent (PreVIEW) periodically.

    While the majority of the Messaging Interface functionality resides on a DOT server, there is a Messaging Interface component resident on the DOA mainframe to accomplish the messaging services required by the legacy applications resident on that system.

16) The CVIEW will be the interface point between the state and the federal SAFER system. State credentialing & safety legacy systems will provide status updates to CVIEW via the Messaging Interface. We will NOT have roadside or credentialing systems communicating directly with federal core systems such as SAFER. CVIEW will serve as the motor carrier summary information database for both inter and intra state carriers.

    Note: The design presumes the use of EDI/post office protocol for the data exchange mechanism with SAFER, although the anticipated FTP/XML exchange facility would be preferred. CVIEW detail design will isolate the exchange facility to the extent possible to minimize rework, in the event the FTP/XML alternative isn't available at the time of Wisconsin's CVIEW development.

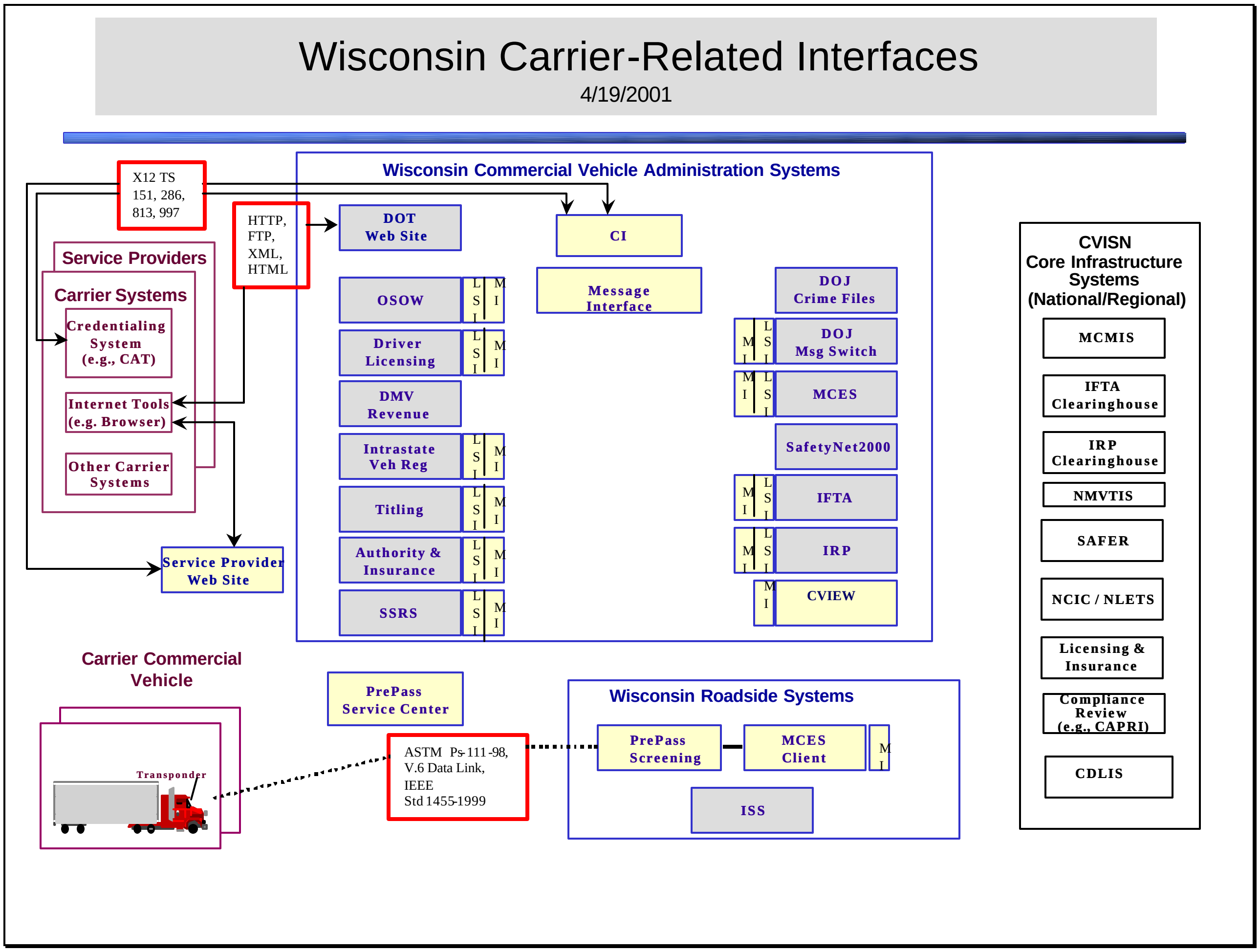
17) The MCES Client will require development. It replaces 3270 configurations which currently provide access to the mainframe based MCES system as well as other state source systems, and to NCIC / NLETS via the DOJ message switch. At minimum, the client will need to handle connectivity to the CVIEW for retrieving and forwarding safety and inspection information & provide roadside connectivity to state systems currently accessible via 3270 connections. We expect it ultimately will connect to the PrePass Screening Computer to obtain the VIN# for Vehicles receiving a pull in signal.

18) The screening component will be supplied by PrePass. PrePass roadside data includes: plate #, Fleet unit number, carrier name, and pass/fail indicators for IFTA, IRP, SSRS, Reg, & ISS. Registered weight available if state requests it. PrePass service center located in Santa Clara, CA will employ an Internet IP connection to roadside PrePass Screening computer to provide updates on screening data. Update interval is every 80 minutes.

    We expect the PrePass Screening computer will ultimately connect to the MCES Client (ROC), and will provide a VIN # for trucks receiving a pull in signal. The MCES Client will use this identifier to make additional snapshot and detail information available to the roadside without manual intervention.

System Interface Summaries

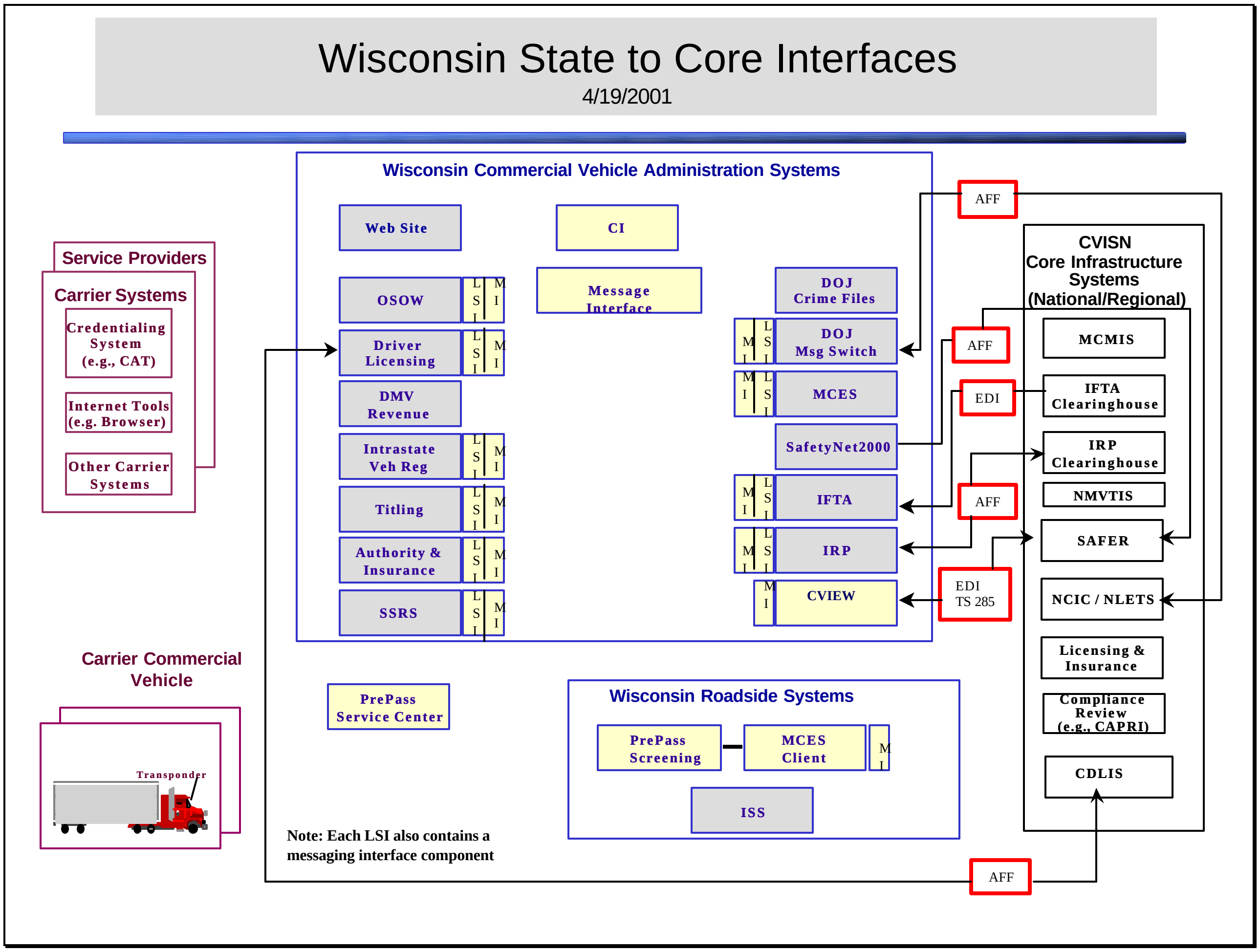
Carrier-Related Interfaces



Wisconsin Carrier-Related Interfaces

4/19/2001

Interfaces Within the State



Wisconsin State to Core Interfaces

4/19/2001

Wisconsin Commercial Vehicle Administration Systems

Web Site

CI

OSOW

Message Interface

DOJ Crime Files

Driver Licensing

DOJ Msg Switch

DMV Revenue

MCES

Intrastate Veh Reg

SafetyNet2000

Titling

IFTA

Authority & Insurance

IRP

SSRS

CVIEW

Service Providers

Carrier Systems

Credentialing System (e.g., CAT)

Internet Tools (e.g. Browser)

Other Carrier Systems

Carrier Commercial Vehicle

Transponder

PrePass Service Center

Wisconsin Roadside Systems

PrePass Screening

MCES Client

ISS

Note: Each LSI also contains a messaging interface component

CVISN Core Infrastructure Systems (National/Regional)

MCMIS

IFTA Clearinghouse

IRP Clearinghouse

NMVTIS

SAFER

NCIC / NLETS

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

AFF

AFF

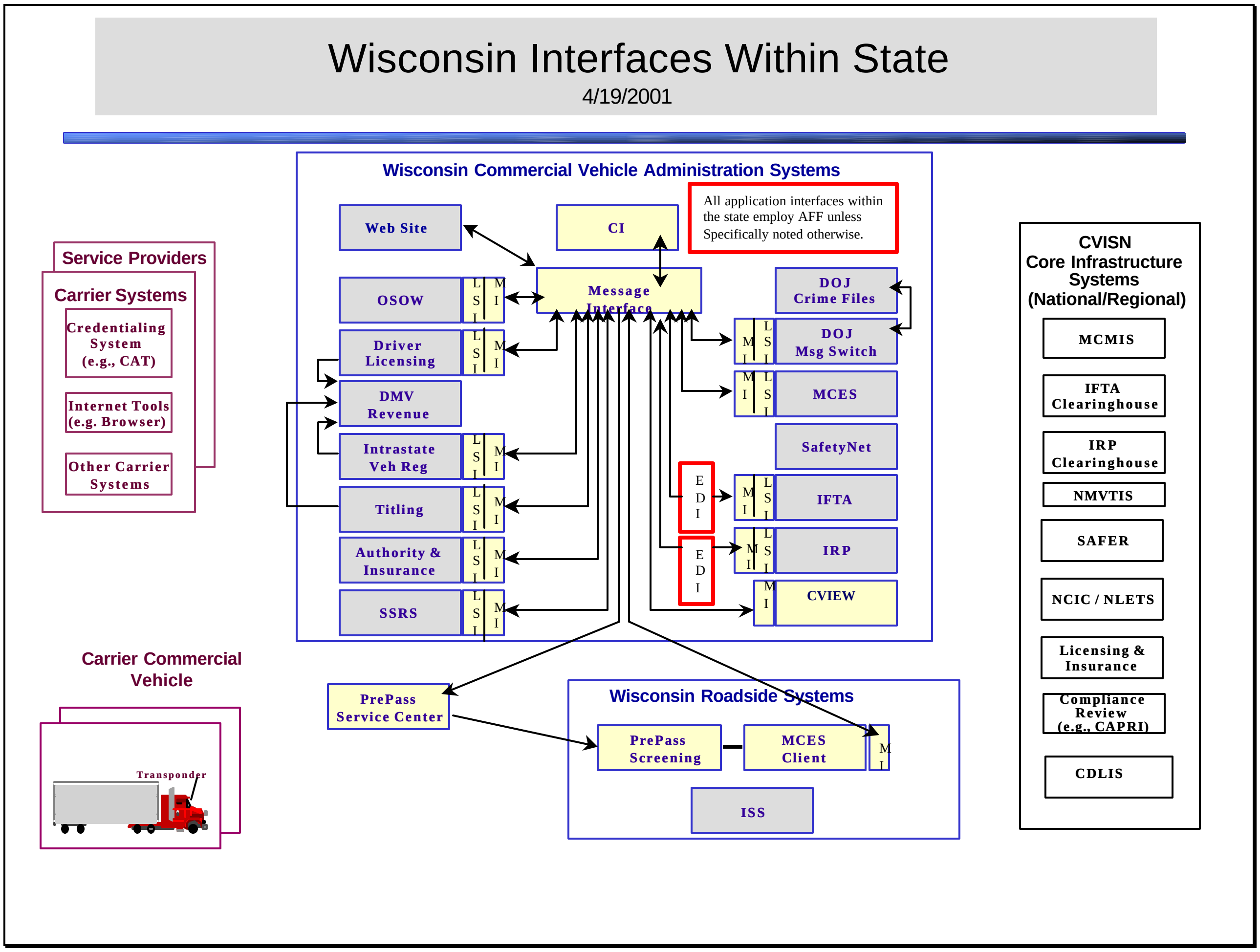
EDI

AFF

EDI TS 285

AFF

State Interfaces with CVISN Core Infrastructure



Wisconsin Interfaces Within State

4/19/2001

Wisconsin Commercial Vehicle Administration Systems

All application interfaces within the state employ AFF unless Specifically noted otherwise.

Web Site

CI

Message Interface

OSOW

Driver Licensing

DMV Revenue

Intrastate Veh Reg

Titling

Authority & Insurance

SSRS

DOJ Crime Files

DOJ Msg Switch

MCES

SafetyNet

IFTA

IRP

CVIEW

L S I

M I

E D I

Service Providers

Carrier Systems

Credentialing System (e.g., CAT)

Internet Tools (e.g. Browser)

Other Carrier Systems

Carrier Commercial Vehicle

Transponder

PrePass Service Center

Wisconsin Roadside Systems

PrePass Screening

MCES Client

ISS

CVISN Core Infrastructure Systems (National/Regional)

MCMIS

IFTA Clearinghouse

IRP Clearinghouse

NMVTIS

SAFER

NCIC / NLETS

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Summary of New Components To Be Added

CI / MI

The Credential Interface (CI) will be the sole state interface point for EDI transactions from carriers and carrier agents. Its principal function is to receive transactions from the carriers or agents, send acknowledgements and products back to the carrier or agent, and provide basic editing for application completeness. It will also provide EDI (eventually XML) translations to and from internal state system formats. Communication among legacy systems internal to the state will continue to use the syntax native to the legacy system. The exception is for vendor-supplied applications such as IRP and IFTA that will use EDI, as well as external interfaces to carrier systems and federal systems.

The Messaging Interface (MI) is closely integrated with the CI and provides messaging and queuing services. Conceptually, the Messaging Interface would have scripts associated with specific application transaction types that would enable it to:

- Receive and store transactions arriving from carriers and carrier agents;
- Spawn transactions to other systems to gather status information needed by a credentialing system to process an incoming transaction;
- Assemble “information packages” (the incoming carrier application transaction, and required status information) and forward to appropriate credentialing system;
- Send acknowledgements and credentialing system products back to carrier or carrier agent;
- Route credentialing system updated status to CVIEW;
- Return detailed credential information in response to an enforcement query from the MCES client;
- Route Snapshots from CVIEW to roadside systems; and
- Route selected Snapshots to PrePass Service Center CVIEW equivalent (PreVIEW) periodically.

CVIEW

The CVIEW will be the interface point between the state and the federal SAFER system. State credentialing & safety legacy systems will provide status updates to CVIEW via the Messaging Interface. We will NOT have roadside or credentialing systems communicating directly with federal core systems such as SAFER. CVIEW will serve as the motor carrier summary information database for both inter and intra state carriers.

MCES Client

The MCES Client provides the functions associated with the Roadside Operations Computer (ROC), i.e. interface to CVIEW to get snapshot data, and to provide roadside access to state source systems. It also, in conjunction with MCES, provides the ASPEN equivalent automated inspection reporting function.

PrePass and Integrated Weigh-In-Motion (WIM)

The PrePass system allows checking motor carrier credentials and weight at highway speeds without stopping the vehicles at inspection stations. As the truck passes over automatic sensors built into the highway, the sensors weigh the vehicle and transmit data to a roadside computer, which verifies that state-required credentials are in order.

The PrePass Screening Computer is a new component to be added. This is supplied as part of the PrePass program. The Screening Computer is used to make the screening decision (pull in or by pass) based on sensor inputs and the snapshot screening criteria. We expect the MCES Client will ultimately connect to the PrePass Screening Computer to obtain the VIN #’s for vehicles receiving a pull in signal. The MCES Client will use these VIN #’s to query state source systems for detail information to be made available to the roadside inspector, without needing to manually key the inquiries.

System Change Summary

Wisconsin has several large projects that need to be completed to accomplish CVISN Level 1 deployment capabilities: CVIEW, CI/MI, MCES Client, and PrePass deployment.

The CVIEW will be constructed using either the current APL version of CVIEW or a vendor's version of CVIEW. In either case, significant amounts of customization will be required.

The CI/MI will be constructed using IBM's MQSeries middleware product. This software is available for every hardware platform that WisDOT uses and ties applications together through the use of message queues.

The MCES Client is primarily a migration effort to convert the existing 3270-based application for use on a workstation. Additional functionality will be added.

PrePass deployment is primarily the responsibility of HELP, Inc. However, there is a considerable amount of coordination involved with other scheduled road building activities.

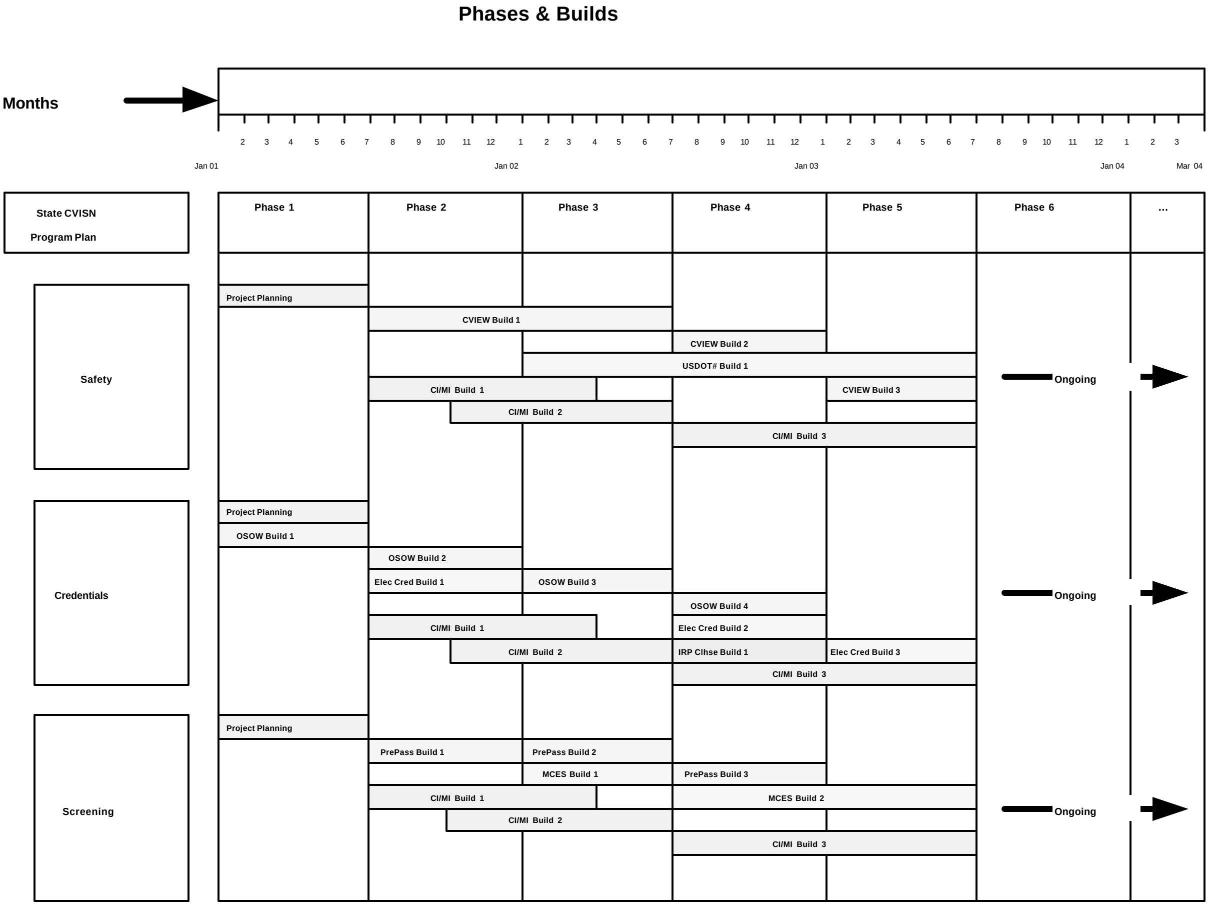
The remaining changes primarily involve creating the connections between the various applications. The following table documents the changes that are believed to be necessary at this time:

System	**No Change**	**Change (S,M,L)**	**New – Build (S,M,L)**	**New – Buy (S,M,L)**
IRP/IFTA to DMV Revenue				M
OSOW Link to DMV Revenue			M	
Web Site			M	
CVIEW			L	
MCES migration to LAN based system		M		
Screening LSI				?
CI / MI			L	
OSOW – LSI / MI		S		
Drivers Licensing – LSI / MI			S	
Intrastate Vehicle Reg – LSI / MI			S	
Authority & Insurance – LSI / MI			M	
SSRS – LSI / MI			M	
DOJ Message Switch – LSI / MI			M	

System	**No Change**	**Change** **(S,M,L)**	**New – Build** **(S,M,L)**	**New – Buy** **(S,M,L)**
MCES – LSI / MI			M	
IFTA COVERSft – LSI / MI				M
IRP Covers – LSI / MI				M
MCES Client – LSI / MI			M	
Titling – LSI / MI			S	
Network Infrastructure	X			
Network Connections		S		
NT Server for CVIEW				S
NT Server for MCES Client (ROC)				S
NT Server for CI / MI				S
IBM MQ Series Software for DOA Mainframe and DOT LAN				M
IP Capability on MDCs				?

Phase Chart

A phase chart is a simplified method of illustrating what activities and deliverables are expected to be accomplished over a period time. Wisconsin's phase chart is predicated on the availability of funding and resources, a situation that does not currently exist. We are ignoring that constraint during the preparation of our plans, but delays in funding or resources will necessarily delay the activities and deliverables.



The following sections briefly describe the projects referenced in the Phases & Builds chart. All time frames are dependent upon funding and resource availability, as well as project prioritization decisions by the Technology Management Council (TMC).

Phase 1 – January 1, 2001 through June 30, 2001

- **Project Planning** – Overall CVISN project planning.
- **OSOW Build 1** – Limited self-issuance of Single Trip permits, using a table based route restriction evaluation routine. Online application for Annual Multiple Trip permits.

Phase 2 – July 1, 2001 through December 31, 2001

- **CVIEW Build 1** – Begin development of a local CVIEW, using existing software available from Johns Hopkins University Applied Physics Lab or other vendor as a framework for our CVIEW.

- **OSOW Build 2** – Online renewals of Annual Multiple Trip permits. Automated faxing of self-issued SS permits. Online inquiry of permit application status. Routing system decision.
- **Electronic Credentialing Build 1** – Provide electronic access to COVERSft, a vendor package from The Polk Company used to process IFTA transactions. The initial functionality will allow a carrier to submit their fuel tax returns.
- **Credential Interface/Message Interface Build 1** – Begin introduction of the IBM MQSeries product into the WisDOT computing environment to serve as the underlying technical infrastructure component for this messaging and queuing application.
- **Credential Interface/Message Interface Build 2** – Begin development of a prototype application to link this messaging interface with a small number of other systems.
- **PrePass Build 1** – Implementation of a PrePass facility at the Hudson, WI SWEF.

Phase 3 – January 1, 2002 through June 30, 2002

- **CVIEW Build 1** – Complete development of a local CVIEW, using existing software available from Johns Hopkins University Applied Physics Lab or a vendor as a framework for our CVIEW.
- **USDOT# Build 1** – Begin modifications to existing systems to add the USDOT number to data files and allow entry and maintenance of the USDOT number.
- **OSOW Build 3** – Acceptance of credit card as payment method. Limited self-issuance of Annual Multiple Trip permits without weight.
- **Electronic Credentialing Build 2** – Provide electronic access to COVERS, a vendor package from The Polk Company used to process IRP transactions. The initial functionality will allow a carrier to apply for supplements.
- **Credential Interface/Message Interface Build 1** – Complete introduction of the IBM MQSeries product into the WisDOT computing environment to serve as the underlying technical infrastructure component for this messaging and queuing application.
- **Credential Interface/Message Interface Build 2** – Complete development of a prototype application to link this messaging interface with a small number of other systems.
- **PrePass Build 2** – Implement snapshot-based PrePass screening.
- **MCES Build 1** – Migrate the current MCES Client from the existing 3270 environment to a LAN-based workstation environment.

Phase 4 – July 1, 2002 through December 31, 2002

- **CVIEW Build 2** – Implement connectivity between CVIEW and SAFER.
- **USDOT# Build 1** – Continue modifications to existing systems to add the USDOT number to data files and allow entry and maintenance of the USDOT number.
- **OSOW Build 4** – Automated Routing. Expand self-issuance of Single Trip permits.
- **Credential Interface/Message Interface Build 3** – Begin expansion of the prototype application to include links with other systems.
- **IRP Clearinghouse Build 1**– Join the IRP Clearinghouse and implement connections between the Polk COVERS application and the clearinghouse.
- **PrePass Build 3** – Implementation of a PrePass facility at the Menomonie, WI SWEF.
- **MCES Build 2** – Begin the connection of the MCES client to CVIEW.

Phase 5 – January 1, 2003 through June 30, 2003

- **CVIEW Build 3** – Add intrastate information to CVIEW.
- **USDOT# Build 1** – Complete modifications to existing systems to add the USDOT number to data files and allow entry and maintenance of the USDOT number.
- **Electronic Credentialing Build 3** – Add increased functionality to electronic access to both the COVERS and COVERSft applications, including the ability to accept electronic payments.
- **Credential Interface/Message Interface Build 3** – Complete expansion of the prototype application to include links with other systems.
- **MCES Build 2** – Complete the connection of the MCES client to CVIEW.

Phase 6 – July 1, 2003 through December 31, 2003 and Beyond

Additional projects will be identified and initiated.

Operational Scenarios

Operation scenarios are a graphical way to describe how a particular activity will be accomplished once CVISN Level 1 deployment is accomplished. A complete set of operational scenarios may be found in Appendix E.

Summary of Wisconsin CVISN Level 1 Conformance

A review of the operational scenarios will show that Wisconsin plans to meet the CVISN Level 1 capabilities in the following ways:

Safety

Wisconsin uses MCES, an ASPEN equivalent, at all major inspection sites. We will deploy a CVIEW to connect to the SAFER database and exchange snapshot information for interstate operators. We will support the standard in place for exchanging information with SAFER. This may be the current EDI standard, but our preference is to use XML for this data exchange. We will use CVIEW as a repository for intrastate carrier and vehicle information.

Credentials

Wisconsin will use a vendor product (Polk COVERSnet) to provide electronic access to the IRP and IFTA systems. We will initially provide a Web interface into these systems, and a computer-to-computer interface using EDI is currently under development. An OSOW system is in production, with additional functionality planned for a phased implementation. Between the IFTA, IRP, and OSOW systems, we expect to accomplish at least 10% of the credentialing volume electronically. Wisconsin is a member of the IFTA Clearinghouse and we intend to join the IRP Clearinghouse.

Screening

Wisconsin plans to implement HELP Inc's PrePass screening and clearance system at two SWEFs. We understand that PrePass is currently developing their own version of CVIEW (PreVIEW) to connect to SAFER and provide snapshot based screening. This will provide interim connectivity to SAFER while we develop our own local CVIEW. We expect to eventually link our CVIEW to PrePass' PreVIEW. We expect that PrePass will follow the DSRC standards and that screening enrollment data will be shared with other PrePass states. The Wisconsin Motor Carriers Association has endorsed PrePass.

Issues

The following issues were identified as part of the CVISN Planning Workshop held in Kissimmee Florida in February 2001:

- We continue to look for funding sources for CVISN deployment with limited success. Without necessary funding, we do not expect to be able to meet CVISN Level 1 compliance by the Congressional target of September 30, 2003.
- Identification of available Federal and State matching funds is challenging.
- Coordination of effort between the DMV Registration Redesign project and the CVISN program is tricky. This can have a significant impact on resource availability and organizational stress.
- Availability of transponder information from non-PrePass enrolled vehicles will require a coordinated effort. According to feedback received at the Planning Workshop, agreements with other transponder administrators would need to be in place before this information could be used.
- Accomplishing end-to-end processing will require some form of electronic payment.
- Resolution of HTE's delivery of the IP Protocol Stack for the Mobile Data Computers is required for connectivity to vehicles.

Contact Information

Additional information about this Top Level Design may be obtained by contacting:

- Jim Anderson, CVISN Project Manager – james.anderson1@dot.state.wi.us
- Barry Larson, CVISN System Architect – barry.larson@dot.state.wi.us

Appendix A – COACH Part 1

Intelligent Transportation Systems (ITS)

Commercial Vehicle Operations (CVO)

CVISN Operational and Architectural Compatibility Handbook (COACH)

Part 1

Operational Concept and Top-Level Design Checklists

Baseline Version

POR-97-7067 V2.0

August 2000

Wisconsin

2. *Guiding Principles*

Statements of principle are being used to document fundamental concepts and guidelines supported by the CVO community. In addition to the specific checklists provided in subsequent sections, these guiding principles provide a top-level checklist of fundamental guidelines for all CVISN activities. CVO stakeholders should ensure that their actions are consistent with these principles. No planning columns are included in the tables for guiding principles since the principles provide guidance rather than specific details that can be scheduled or measured.

The guiding principles were developed under the auspices of the ITS America CVO Program Subcommittee [References 17, 18, 19]. These principles continue to be under review by ITS America and the US Department of Transportation. They will be updated as required to reflect the consensus of the CVO community. The current principles are copied verbatim into the tables in this chapter.

2.1 ITS/CVO Guiding Principles [Reference 17]

"The ITS America CVO Committee presents this set of guiding principles which will guide the states and federal government on matters concerning technology and commercial vehicle operations. This list of 39 guiding principles was established by the CVO Programs Subcommittee with representation from National Private Truck Council, ATA, carriers, owner operators, motorcoach representation, UPS, several state administrative and regulatory agencies, AAMVA, AASHTO, and Canada. These principles took two years to create and 100% consensus was reached.

2.1.1 ITS/CVO Guiding Principles : Summary

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	1.	A **balanced approach** involving ITS/CVO technology as well as institutional changes will be used to achieve measurable improvements in efficiency and effectiveness for carriers, drivers, governments, and other CVO stakeholders. Specific technology and process choices will be largely **market-driven**.	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	2.	The CVISN architecture will enable **electronic information exchange** among authorized stakeholders via open standards.	
F	3.	The architecture **deployment will evolve incrementally**, starting with legacy systems where practical and proceeding in manageable steps with **heavy end-user involvement**.	
F	4.	Safety assurance activities will **focus resources on high risks**, and be structured so as to reduce the compliance costs of low-risk carriers and drivers.	
F	5.	Information technology will support improved practices and procedures to **improve CVO credential and tax administration efficiency** for carriers and government.	
F	6.	Roadside operations will **focus on eliminating unsafe and illegal operations by carriers, drivers, and vehicles** without undue hindrance to productivity and efficiency of safe and legal carriers and drivers.	

2.1.2 ITS/CVO Guiding Principles: General CVO

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	1.	To the extent possible, ITS/CVO technology development and deployment will be **market-driven**. The federal role in ITS deployment will be limited to instances in which a government role is indispensable and in which the technology is proven and reliable.	If market-driven means up to state and local agencies as well as motor carriers.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	**2.**	**Investment and participation** in ITS/CVO technology will be **voluntary**.	
F	3.	The relative benefits of various ITS/CVO technology applications and investments will be assessed quantitatively using **measures of effectiveness** and established methods of quality control.	
F	4.	Potential ITS/CVO technology applications will be evaluated against regulatory choices involving low-technology and non-technological options to ensure applications are **cost-effective for both government and industry**.	
P	5.	Government CVO policies and regulatory practices will permit safe and legal carriers and drivers to operate without **unnecessary regulatory and administrative burdens**.	Unnecessary is an ambiguous term. Some states see SSRS as unnecessary, others feel it is required.
F	6.	Stakeholders will use **technology and institutional reform** to implement continuous process improvement and cost-effective process re-engineering.	
F	7.	The **confidentiality** of proprietary and other sensitive stakeholder information will be preserved.	
F	8.	The United States CVO community will work to implement **compatible policies** and architecture and **interoperable systems** in all states.	
F	9.	The United States CVO community will work with those in Canada, Mexico, and other nations to encourage **compatible policies** and architecture and to implement **interoperable systems** throughout North America and, when possible, worldwide.	

2.1.3 ITS/CVO Guiding Principles: CVISN Architecture

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	1.	The CVISN architecture will be **open**, modular, and adaptable.	
F	2.	The architecture will enable **data exchange** among systems, a key to reaching CVO objectives. Methods used to exchange data will ensure **data integrity and prevent unauthorized access**.	
F	3.	Data exchange will be achieved primarily via **common data definitions**, message formats, and communication protocols. These enable development of interoperable systems by independent parties.	Message formats and protocols internal to state will be at states discretion.
F	4.	A jurisdiction shall have and maintain **ownership of any** data collected by any agent on its behalf.	
F	5.	The architecture will accommodate **existing** and near-term **communications** technologies.	
F	6.	The architecture will accommodate **proven technologies and legacy systems** whenever possible.	
F	7.	The CVISN architecture will allow government and industry a **broad range of options**, open to competitive markets, in CVO technologies.	

2.1.4 ITS/CVO Guiding Principles: CVISN Deployment

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	1.	The feasibility of the **architecture will be demonstrated incrementally** in simulations, prototypes, operational tests, and pilots. There will be **heavy end-user involvement** in each step of the process.	
F	2.	After feasibility has been demonstrated, key architectural elements will be incorporated into appropriate national and international **standards**.	
F	3.	The architecture **deployment will evolve incrementally**, starting with legacy systems where practical and proceeding in manageable steps.	
F	**4.**	**Strong federal leadership** will foster voluntary cooperative efforts within government jurisdictions and among groups of other stakeholders to develop systems which are in accord with the architecture.	

2.1.5 ITS/CVO Guiding Principles: Safety Assurance

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	**1.**	**Carriers and drivers will be responsible** for the safe and legal operation of commercial vehicles.	
F or P	2.	Jurisdictions will develop and implement **uniform standards, practices, procedures, and education programs** to improve safety. These activities will leverage market forces that encourage safety.	What does "leverage market forces" mean?

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
P	3.	Jurisdictions **will focus** safety **enforcement** resources **on high risk** carriers and drivers. They will remove chronic poor performers from operation and help cooperative marginal performers to improve.	Where able to due to resources/ jurisdictions. "Remove chronic poor performers" sounds like PRISM.
F	4.	Jurisdictions will conduct **inspections** and **audits** to provide **incentives** for carriers and drivers to improve poor performance and to collect information for assessing carrier and driver performance.	
P	5.	Jurisdictions will use a **safety risk rating** for all carriers based on best available information and common criteria.	Doing it for interstate – working on a system for intrastate.
F	6.	Jurisdictions will identify **high risk drivers** based on best available information and common criteria.	
P	7.	Safety programs will provide **benefits which exceed costs** for carriers and drivers as well as governments.	Safety in and of itself is a benefit which exceeds costs, but if carriers are only concerned with their bottom line, they will not see it that way.

2.1.6 ITS/CVO Guiding Principles: Credentials & Tax

Commit Level (F/P/N)	Item ##	Compatibility Criteria	Comments
F	**1.**	**Electronic information** will be used in place of paper documents for the administration of CVO credential and tax requirements.	Paper credentials will still be required.
F	2.	Authorized users will be able to electronically exchange credential and tax-related information and funds via **open standards** and transmission options.	
F	3.	The information needed to administer tax and credential programs involving carriers, drivers, and vehicles will be **available to authorized officials**, on a need-to-know basis.	
F	4.	Individual jurisdictions, or their designated agent, will be the **authoritative source** of information on credentials they issue.	

2.1.7 ITS/CVO Guiding Principles: Roadside Operations

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
P	1.	Roadside operations will **focus on eliminating unsafe and illegal operations by carriers, drivers, and vehicles** and will be designed and administered to accomplish this in a manner that does not unduly hinder the productivity and efficiency of safe and legal motor carriers and drivers.	What is “unduly hinders”? Their definition could be different than enforcement’s.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
P	2.	Jurisdictions will support CVO roadside operations programs with **timely, current, accurate, and verifiable electronic information**, making it unnecessary for properly equipped vehicles to carry paper credentials."	Not all sites will be equipped – at least initially – and portable operations will not be equipped.

2.2 Fair Information Principles for ITS/CVO [Reference 18]

"*These fair information principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Technical Committee.*

These principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop fair information and privacy guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the fair information principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***FIP #1***	***Privacy*** The reasonable expectation of privacy regarding access to and use of personal information should be assured. The parties must be reasonable in collecting data and protecting the confidentiality of that data.	Full commitment but following our open records law. This is a critical element given the privacy concerns in Wisconsin political arena.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***FIP #2***	***Integrity*** Information should be protected from improper alteration or improper destruction.	
F	***FIP #3***	***Quality*** Information shall be accurate, up-to-date, and relevant for the purposes for which it is provided and used.	
F	***FIP #4***	***Minimization*** Only the minimum amount of relevant information necessary for ITS applications shall be collected; data shall be retained for the minimum possible amount of time.	
F	***FIP #5***	***Accountability*** Access to data shall be controlled and tracked; civil and criminal sanctions should be imposed for improper access, manipulation, or disclosure, as well as for knowledge of such actions by others.	This is a critical element given the privacy concerns in Wisconsin political arena.
F	***FIP #6***	***Visibility*** There shall be disclosure to the information providers of what data are being collected, how they are collected, who has access to the data, and how the data will be used.	
F	***FIP #7***	***Anonymity*** Data shall not be collected with individual driver identifying information, to the extent possible.	
F	***FIP #8***	***Design*** Security should be designed into systems from the beginning, at a system architecture level.	
F	***FIP #9***	***Technology*** Data encryption and other security technologies shall be used to make data worthless to unauthorized users.	No DOT standard so in theory yes, but in practice unsure. Encryption would be used in transmitting certain data, certainly wouldn't encrypt databases.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***FIP #10***	***Use*** Data collected through ITS applications should be used only for the purposes that were publicly disclosed.	
F	***FIP #11***	***Secondary Use*** Data collected by the private sector for its own purposes through a voluntary investment in technology should not be used for enforcement purposes without the carrier's consent.	

Date approved by the Board of Directors: April 22, 1999

Note: These guiding principles address only issues of privacy and data control. They do not address all issues related to concepts of operations or interoperability. These issues are addressed in separate guiding principles."

2.3 ITS/CVO Interoperability Guiding Principles [Reference 19]

"These interoperability guiding principles were prepared in recognition of the importance of promoting interoperability in the implementation of Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Technical Committee.

These principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop interoperability guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the interoperability principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for assuring interoperability in their contracts and agreements.

2.3.1 ITS/CVO Interoperability Guiding Principles: General

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***IGP #1***	The CVO community will work to implement interoperable ITS/CVO systems in all United States jurisdictions.	
F	***IGP #2***	The CVO community will work with the CVO communities in Canada and Mexico to implement interoperable ITS/CVO systems throughout North America.	Issue could be standards.
F	***IGP #3***	The CVO community will work to ensure that ITS/CVO systems, where appropriate, are interoperable with other ITS systems (e.g., electronic toll systems).	
F	***IGP #4***	Interoperable ITS/CVO systems will be achieved through the development, adoption, and adherence to common standards for hardware, systems/software, operations, and program administration.	
F	***IGP #5***	Each jurisdiction will support the national ITS/CVO information system architecture and data exchange standards developed under the Commercial Vehicle Information Systems and Networks (CVISN) program.	
F	***IGP #6***	Transponders shall have a unique identifier.	Not sure if needed. Like a VIN#? What does this have to do with us?
F for all except 7a, which is P	***IGP #7***	Information systems supporting electronic screening, credentials administration, and safety assurance will use: 7a. US DOT numbers for the identification of both interstate and intrastate motor carriers. 7b. Commercial Drivers License (CDL) numbers for the identification of commercial drivers. 7c. Vehicle Identification Numbers (VIN) and license plate numbers for the identification of power units.	Intrastate carriers may not have this requirement (references 7a). Are we looking to put this in a transponder? I don't think so at this time (references 7b).

2.3.2 ITS/CVO Interoperability Guiding Principles: Hardware

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***IGP #8***	Commercial vehicle operators will be able to use one transponder for power unit-to-roadside communications in support of multiple applications including electronic screening, safety assurance, fleet and asset management, tolls, parking, and other transaction processes.	We have no input into toll road, fleet and asset management, parking, etc.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***IGP #9***	Public and public-private DSRC applications will support open standards that are consistent with the national ITS architecture.	Can't speak for the public – private side.

2.3.3 ITS/CVO Interoperability Guiding Principles: Systems/Software

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***IGP #10***	Public and public-private organizations will support open data exchange standards for the state-state, state-federal, state-provincial, and carrier-agency exchange of safety and credentials information as described in the national ITS architecture.	Same as previous comment – when private is added – also adding provincial to the mix. What are their requirements & how do they mesh with ours?

2.3.4 ITS/CVO Interoperability Guiding Principles: Operations

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
F	***IGP #11***	Jurisdictions will support common standards for placement of DSRC transponders on trucks and buses to ensure the safe and cost-effective use of transponders.	We don't check buses at our facilities.
F	***IGP #12***	Jurisdictions will support a common set of recommended practices concerning the selection, layout, and signage of roadside screening sites (i.e., weigh stations, ports-of-entry, international border crossings, and temporary inspection sites) to ensure safe operations.	Mobile operations may not conform to "common set" of practices – depends what they are.
F	***IGP #13***	Jurisdictions will support a common performance standard for roadside electronic enforcement screening and passage of transponder-equipped motor carriers to ensure equity in enforcement.	There will likely be some criteria differences between states. Can support common minimum standard – but some states may want to add more.
F	***IGP #14***	Roadside electronic enforcement screening criteria will include the following: motor carriers must be enrolled in the jurisdiction's program; must meet the jurisdiction's enrollment criteria; and must meet all legal requirements established by the jurisdiction.	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Comments
N	***IGP #15***	Jurisdictions will support quarterly reviews of carrier qualifications to ensure that the standards evolve to meet the changing needs of government and motor carriers.	This could take a substantial amount of resources. Who will do quarterly reviews – who rules on the "evolving standards". We have several different interpretations of this, and are not comfortable with any of them. CVISN is on-going – why quarterly reviews? Quarterly reviews are not realistic just to see if a carrier is keeping up-to-date. Evolving standards is a whole different issue.
F	***IGP #16***	A jurisdiction will not retain the identification codes or other data from the DSRC transponders of passing motor carriers who are not enrolled in the jurisdiction's program.	Not sure if need for traffic accident questions or other State Patrol needs. May find a need to keep some of the data – other programs may need this.
F or P	***IGP #17***	Jurisdictions will support a common performance standard for selection of vehicles and drivers for roadside safety inspection.	State policies will make this challenging. Jurisdictions may choose different performance standards based on regional need.
F	***IGP #18***	Jurisdictions will support a common performance standard for recording and reporting roadside safety inspection results.	Could support common "minimum" performance standard but some may want more based on their need.
F	***IGP #19***	Jurisdictions will support a common performance standard for reconciling disputed roadside safety inspection results.	Depends on the standard – again may have regional need. We support this at a high level, subject to the laws and regulations of the jurisdiction.

2.3.5 ITS/CVO Interoperability Guiding Principles: Program

Commit Level (F/P/N	Item #	Compatibility Criteria	Comments
F	***IGP #20***	Motor carrier participation in ITS/CVO roadside electronic screening programs will be voluntary; motor carriers will not be required to purchase or operate DSRC transponders.	

Commit Level (F/P/N	Item #	Compatibility Criteria	Comments
F	***IGP #21***	Motor carriers will have the option of enrolling in any ITS/CVO roadside electronic screening program.	Must be inter-operable.
F	***IGP #22***	Jurisdictions will support uniform criteria for enrollment of motor carriers in ITS/CVO roadside screening programs.	Already have international plans/standards for participation. I support the concept – depends on what the criteria is.
F	***IGP #23***	Enrollment criteria will include consideration of safety performance and credentials status (e.g., registration, fuel and highway use taxes, and insurance).	
F	***IGP #24***	No jurisdiction will be required to enroll motor carriers that do not meet the criteria for enrollment.	
F	***IGP #25***	Motor carriers may obtain a DSRC transponder from the enrolling jurisdiction or a compatible DSRC transponder from an independent equipment vendor of the motor carrier's choice.	
F	***IGP #26***	Each jurisdiction will determine the price and payment procedures, if any, for motor carriers to enroll and participate in its ITS/CVO electronic screening program.	
F	***IGP #27***	Jurisdictions shall work to establish business interoperability agreements among roadside electronic screening programs.	
F	***IGP #28***	A jurisdiction will make a motor carrier's DSRC transponder unique identifier available to another jurisdiction upon written request and authorization by the motor carrier.	Depends on certain criteria or reason for request.
F	***IGP #29***	Jurisdictions will work toward development of a single point of contact for motor carriers enrolling in more than one ITS/CVO roadside screening program.	

Commit Level (F/P/N	Item #	Compatibility Criteria	Comments
F	***IGP #30***	Each jurisdiction will fully disclose and publish its practices and policies governing, at a minimum: 30a. Enrollment criteria; 30b. Transponder unique identifier standards; 30c. Price and payment procedures for transponders and services; 30d. Screening standards; 30e. Use of screening event data; and 30f. Business interoperability agreements with other programs."	

Date approved by the Board of Directors: April 22, 1999

Note: These guiding principles address only issues of interoperability. They do not address all issues related to concepts of operations or privacy and data control. These issues are addressed in separate guiding principles."

3. State Institutional Framework

The checklist in this section summarizes the institutional and business planning steps that states should take to become ready to implement the CVISN architecture and concepts. The checklist is based on the ideas outlined in the January 1999 letter from the Director, Office of Motor Carrier Safety & Technology on CVISN Workshops [Reference 23] and the CVISN Model Deployment Request for Information and Request for Application [References 21-22].

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
N	1.	The State has contacted or has plans to contact State and local transportation officials to explore potential joint-uses of transponders and ensure integration among multiple applications (i.e., CVO, toll, traffic probes, parking management, etc.)	L1 CRF 1155	We have no input into toll road, fleet and asset management, parking, etc.
?	2.	The State has evaluated or has plans to evaluate the data that is being collected for CVISN initiatives to determine if other State and local transportation entities (e.g., traffic management center) outside the CVO community could use the data which is collected under CVISN deployment, consistent with data privacy agreements.	L1 CRF 1155	
F	3.	The State has conducted or has plans to conduct outreach to its motor carrier partners about metropolitan and rural ITS initiatives within the State that could provide benefits to its motor carrier operations. Examples of these initiatives include web sites on roadway weather information systems, incident management systems, and traffic management systems.	L1 CRF 1155	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	4.	The State is committed to complete the full cycle of the workshops, and upon completion, to begin deployment of the ITS/CVO systems and services that meet the unique economic, administrative, and transportation needs, as outlined in the State ITS/CVO Business Plan.	L1	Subject to resource availability.
F	5.	A qualified core project team that will participate in all three of the workshops has been identified. This project team must include the following individuals: the State's CVISN project manager; the State's CVISN system architect; a project facilitator/administrator, who could be a representative of a participating State agency or a consultant working with the State; operations staff representing the agencies responsible for the State's major CVO functional areas (i.e., IRP, IFTA, safety information systems, roadside safety inspections, size and weight enforcement, and credentials enforcement); staff from the State department of information technology or comparable information technology units within the State CVO agencies; representative of the State Department of Transportation; representatives of the FMCSA and FHWA Division office; and a motor carrier industry representative (invited). See Reference 23 for qualification details.	L1	
N	6.	Appropriate and sufficient staff, equipment, and State and private funding are available to carry out the deployment of CVISN and ITS/CVO services. The CVISN project has sufficient priority (i.e., other higher-priority projects are not competing for the same resources).	L1	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	7.	A State CVO strategic plan and/or business plan exists and has been accepted by the FHWA (or FMCSA). It outlines the goals, strategies, anticipated benefits and costs, organization, projects, schedules, and resources relevant to achieving the envisioned CVO environment.	L1	
F	8.	A planning and coordination process exists which includes all State agencies involved in any aspect of motor carrier safety and regulation.	L1	Not formal.
P	9.	The top executives and chief information systems managers of each involved agency have endorsed State CVO plans and given the CVISN project manager adequate authority.	L1	
F	1	A process for resolution of conflicts among participating agencies exists.	L1	
F	1	State agencies have a strong commitment to customer service and the ability to work with the motor carrier industry in their State.	L1	
F	1	State agencies involve the motor carrier industry in the planning process.	L1	
F	1	State agencies conduct education programs to improve the safety performance and regulatory compliance of motor carriers.	L1	Compliance reviews are conducted with motor carriers, as well as education programs.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	1	State agencies provide periodic forums for obtaining suggestions and concerns from the motor carrier industry.	L1	
F	1	State agencies actively pursue opportunities for and implement business process reengineering projects.	L1	
F	1	An e-mail system is available among agencies.	L1	
F	1	At least key agency staff members have access to the Internet.	L1	
F	1	The State has adopted an open standard (ANSI ASC X12, for example) for electronic data interchange with the public.	L1	
F	1	The State's communications infrastructure is sufficiently developed to extend to the kinds of exchanges needed under the CVISN Architecture.	L1	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
P	2	There are no State legislative barriers relative to data privacy, physical signature requirements, data exchange among agencies, data exchange with other states, or other uses of information technology required to implement the CVISN concept of operations.	L1	Some issues remain.
F	2	The legislature provides adequate resources to support an active ITS/CVO program and deployment of the ITS/CVO services.	L1	
F	2	The State participates in one or more regional CVO forums to assist in developing regional and national interoperable systems and compatible policies and procedures.	L1	
F	2	The State is willing to provide timely, electronic information to the planned clearinghouses to support the base state agreements.	L1	Yes, we are willing.
F	2	The project team has completed the ITS/CVO technical training courses. The first course, Introduction to ITS/CVO, is recommended for workshop participants but can be waived for personnel with prior ITS/CVO knowledge and experience. The second course, ITS/CVO Technical Project Management for Non-Technical Managers, and third course, Understanding ITS/CVO Technology Applications, are required for the personnel who will represent each State at the workshops.	L1	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
	~~2~~	~~The State has identified and made adequate progress towards the resolution of any Y2K problems among CVO agencies. It is strongly recommended that States resolve any Year 2000 computer problems among CVO agencies before beginning the workshops.~~	~~L1~~	No longer applicable.
F	2	Effective procurement plans and processes are in place to acquire services and equipment needed to support the CVISN project, and the CVISN team is aware of constraints the processes impose.	L1	RFP process is both lengthy & difficult.
F	2	Effective subcontract management processes are in place and allow timely identification and resolution of performance problems.	L1	We deal with a prime contractor. Subcontractors are their problem.
P	2	The CVISN team has a clear understanding of the State-specific requirements for information technology projects, e. g., whether or not a feasibility study is required.	L1	BAS review process & DOT "page 1" process not clear to other divisions.
F	2	The CVISN team has a clear understanding of the State-specific budget cycles and is aware of constraints they impose.	L1	

4. State Systems Checklists

The checklists in this chapter describe operational concepts and top-level requirements. The tables are divided into these categories:

- General
- CV Administration
- Safety Information Exchange and Safety Assurance
- Electronic Screening

Operational concepts and top-level requirements in the “general” category apply to the other three categories.

For each category there are two tables.

- The first table in each category lists Operational Concepts. The concepts are based on an interpretation of the guiding principles and the state of existing and emerging technologies today. The elements in each table in this section were originally based on the Key Operational Concepts sections of the OCD [Reference 9]. Updated versions of the operational concepts are included in the CVISN Guide to Top-Level Design [Reference 13] and in the CVISN Guides to Safety Information Exchange, Credentials Administration, and Electronic Screening [References 14-16]. This version of the COACH reflects the updated concepts.
- The second table in each category lists top-level requirements for the design of state systems. The tables show more detail about what “CVISN Level 1” means. The CVISN Level 1 requirements are marked with “L1” in the fourth column (Req Level (L1/E/C)). For an overview of CVISN Level 1, see the Introductory Guide to CVISN [Reference 12].

4.1 General Operational Concepts and State Systems Design Requirements

The general state system design requirements apply to **all** state systems. They facilitate interoperability and the exchange of information within a single state, and across jurisdictions. These requirements apply to safety, credentialing, and electronic screening systems.

CRF 1048 authorized updating CVISN documents to reflect FMCSA's new policy on credentials administration. The policy change resulted from analyzing the results of a survey about electronic credentialing interactions between motor carriers and state information systems (see Reference 38). The new policy is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.
- FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.
- FMCSA encourages the exploration of XML as an alternative to EDI.

This is a policy regarding CVISN Level 1. If a state chooses to implement only a person-to-computer credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state chooses to implement only a computer-to-computer credentialing approach, then implementation of a person-to-computer interface is considered an Enhanced capability. The tables in this section have been updated accordingly.

The concepts in the following table are based on an interpretation of the guiding principles and the state of existing and emerging technologies today. The elements in this table were originally based on the Key Operational Concepts sections of the OCD [Reference 9]. Updated versions of the operational concepts are included in the CVISN Guide to Top-Level Design [Reference 13] and in the CVISN Guides to Safety Information Exchange, Credentials Administration, and Electronic Screening [References 14-16]. This version of the COACH reflects the updated concepts.

Table 0-1 General Operational Concepts

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	1.	Good business processes can be enhanced through improved automated access to accurate information.	L1	
F	2.	Authoritative sources are responsible for maintaining accurate information. Each jurisdiction participating in ITS/CVO information exchange identifies the authoritative source for each data item.	L1	
F	3.	Sometimes it is practical for authoritative systems to authorize indirect sources to assist in the information exchange process.	L1	
F	4.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying carriers must be adopted. The Primary Carrier ID should be used in interface agreements (open standards, Internet-based exchanges, and custom interface agreements) to facilitate the exchange of carrier information. How the ID is stored internally outside the interface is up to the system implementers. The ID should be based on the USDOT number for both interstate and intrastate carriers. If it is not feasible for the state to use USDOT number as the ID type for all intrastate carriers, then the state should establish some convention for the Primary Carrier ID that will apply to all intrastate carriers in that state.	L1 – interstate C – intrastate	
F	5.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying drivers must be adopted for interstate and intrastate operators. The Commercial Drivers License (CDL) number should be the basis of the Driver ID.	L1	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	6.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying vehicles must be adopted for interstate and intrastate operators. The Vehicle Identification Numbers (VIN) and jurisdiction plus license plate numbers should be the bases for the identification of power units.	L1	
F	7.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying international trips must be adopted. The Trip/Load number consisting of DUNS and trip-specific ID should be the basis for identifying international trips.	E	
F	8.	Standard information exchange is supported via carrier and vehicle (and eventually driver) snapshots.	L1 – carrier & vehicle C – driver	
F	9.	Flexible implementation/deployment options are accommodated by the ITS/CVO architecture. As technology changes, so will the architecture.	L1	
F	10.	Open standards are used for interchanges between public and private computer systems. Today, ANSI ASC X12 EDI transactions are used for some carrier-state information systems' interactions. We anticipate that XML will be also used in the future. DSRC standards for the messages, data link, and physical layers are used for vehicle-roadside interactions.	L1 CRF 1048 CRF 1164	
F	11.	Enhanced data exchange will allow all activities to focus resources on high risk operators.	L1	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	12.	Interoperability is assured by a process of architecture conformance checks throughout a project's lifecycle, culminating in execution of standardized interoperability tests. If a tested system is changed, the interoperability tests are re-run as part of the re-validation process.	L1	
F	13.	The Fair Information Principles for ITS/CVO will be implemented using a combination of policies, procedures, technology, and training. Stakeholders will be included in the discussions of the techniques to be used to implement the principles.	L1	
F	14.	Citations are based on a review of real-time conditions and checks with authoritative sources.	L1	
F	15.	The Internet is used as a wide area network for information exchange.	L1 CRF 1084	
F	16.	The World Wide Web is used for interactions and information exchanges between private people and government systems (e. g., for credentials applications or commercial vehicle regulations).	L1 CRF 1048 CRF 1164	
F	17.	The focus is on sharing data among safety, credentialing and screening processes. The CVISN Program is structured to encourage states to design and deploy these three elements in parallel.	L1 CRF 632	

The top-level requirements in the following table apply to the design of all state systems. The table shows more detail about what "CVISN Level 1" means. The CVISN Level 1 requirements are marked with "L1" in the fourth column (Req Level (L1/E/C)). For an overview of CVISN Level 1, see the Introductory Guide to CVISN [Reference 12].

Table 0-2 General State Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.1.1**	Adopt standard identifiers for carriers, vehicles, drivers, and transponders to support information exchange.	L1				
F	1	Adopt standard identifiers for interstate carrier, vehicle, driver, and transponder.	L1				
F	2	Adopt standard identifiers for intrastate carrier, vehicle, driver, and transponder.	C				
F	**4.1.2**	Use the World Wide Web for person-to-computer interactions between private citizens and state information systems.	L1;E CRF 1048 CRF 1164				See the note about CRF 1048 for credentialing, above.
F	**4.1.3**	Use open standards for computer-to-computer exchange of information with other jurisdictions and with the public.	L1; E CRF 1048 CRF 1164				See the note about CRF 1048 for credentialing, above.
F	1	Use ANSI X12 EDI standards for transactions between state information systems and private systems (CV operators, insurance companies, etc.).	L1; E				See the note about CRF 1048 for credentialing, above; EDI is recommended in the near term.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	2	Use ANSI X12 EDI standards for transactions between state information systems and CVISN Core Infrastructure systems, where available.	L1; E				See the note about CRF 1048 for credentialing, above; EDI is recommended in the near term.
P	3	Use XML standards for transactions between state information systems and private systems (CV operators, insurance companies, etc.) (contingent on demonstration of feasibility).	E				Need to see standards and understand process before full commitment.
F	**4.1.4**	Ensure that all information transfers, fee payments, and money transfers are authorized and secure.	L1				
F	**4.1.5**	Exchange safety and credentials data electronically within the state to support credentialing, safety, and other roadside functions. Where useful, exchange snapshots.	L1				
F	1	Data for interstate carriers	L1				
F	2	Data for interstate vehicles	L1				
F	3	Data for intrastate carriers	E				
F	4	Data for intrastate vehicles	E				
F	5	Data for drivers	C				
F	**4.1.6**	Demonstrate technical interoperability by performing Interoperability Tests.	L1				
F	**4.1.7**	Support electronic payments.	E				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
P	**4.1.8**	Receive, collect, and archive relevant CVO data for historical, secondary, and non-real-time uses.	E CRF 1047				Subject to Wisconsin's privacy interpretation.

4.2 State Safety Information Exchange and Safety Assurance Systems Design Requirements

The state safety information exchange and safety assurance systems are likely to consist of:

- Inspection (e.g., ASPEN)
- SAFETYNET
- Citation & Accident
- Compliance Review (e.g., CAPRI (Compliance Analysis Performance Review Information))
- CV Information Exchange Window (CVIEW)

The state CV safety information exchange and safety assurance systems will operate at one or more (generally) fixed locations within a state. The systems perform safety information exchange and safety assurance functions supporting safety regulations. States may form regional alliances to support these functions. Each state coordinates with other states, regional alliances, and CVISN Core Infrastructure systems to support nationwide access to safety information for administrative and enforcement functions.

The concepts in the following table are based on an interpretation of the guiding principles and the state of existing and emerging technologies today. The elements in this table were originally based on the Key Operational Concepts sections of the OCD [Reference 9]. Updated versions of the operational concepts are included in the CVISN Guide to Top-Level Design [Reference 13] and in the CVISN Guide to Safety Information Exchange [Reference 14]. This version of the COACH reflects the updated concepts.

Table 0-3 Safety Information Exchange and Safety Assurance Operational Concepts

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
P	1.	Data are collected to quantify the primary measures of effectiveness related to safety of CVO (accidents and fatalities).	L1	Depends on what data can be collected -/ used.
P	2.	Electronic safety records (snapshots) are made available at the roadside to aid inspectors and other enforcement personnel.	L1	Not available to mobile operations.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
P	3.	Inspectors use computer applications to capture, verify, and submit intrastate and interstate inspection data at the point of inspection.	L1	Mobile cannon submit at the time of inspection currently.
P	4.	Safety data are made available electronically to qualified stakeholders.	L1	
F	5.	User access to data is controlled (restricted and/or monitored) where necessary.	L1	
F	6.	Mechanisms are made available for operators to dispute safety records held by government systems.	L1	
P	7.	Compliance reviews are supported through electronic access to government-held safety records.	E	Not available for intrastate at this time.
F	8.	Safety risk ratings are determined according to uniform guidelines.	E	
P	9.	Jurisdictions support a standard set of criteria for inspection selection.	E	What if they want to include more criteria?
P	10.	A comprehensive safety policy, including roadside and deskside activities, is implemented to improve safety.	C	What does “comprehensive” mean here?
	11.	Carriers are associated with a base state for safety information record storage and credentialing.	C	
	12.	Compliance reviews are supported through electronic access to carrier-held records.	C	

The top-level requirements in the following table apply to the design of state safety-related systems. The table shows more detail about what "CVISN Level 1" means. The CVISN Level 1 requirements are marked with "L1" in the fourth column (Req Level (L1/E/C)). For an overview of CVISN Level 1, see the Introductory Guide to CVISN [Reference 12].

Table 0-4 State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.2.1**	Use ASPEN (or equivalent) at all major inspection sites	L1				
F	1	Select vehicles and drivers for inspection based on availability of inspector, standard inspection selection system, vehicle measures, and random process, as statutes permit.	L1				
F	2	Report interstate inspections to MCMIS via SAFETYNET	L1				
F	3	Report intrastate inspections to SAFETYNET	L1				
P	4	Submit interstate and intrastate inspections for 45-day storage to SAFER.	L1				Depends on capability of SafetyNet 2000.
F	5	Periodically check OOS orders issued in the state to focus enforcement and safety assurance activities.	E				
F	6	To assist in inspection, use DSRC to retrieve summary vehicle safety sensor data, if driver allows and vehicle is properly equipped.	C				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
P	7	To assist in inspection, use DSRC to retrieve driver’s daily log, if driver allows and vehicle is properly equipped.	C				Our training & ability.
P	8	Use electronically-generated driver’s daily log, if driver offers as an alternative to a manually-maintained log during an inspection.	C				Requires training of inspectors – some may not be properly trained.
F	**4.2.2**	SAFETYNET 2000 submits interstate and intrastate inspections reports to SAFER.	L1				As soon as we have it.
	4.2.3	Maintain snapshots (or equivalent information) for operators based in the state and make available to within-state information systems and users.	E CRF 827				
F	1	For any given snapshot, there is only one authoritative source (or group of authoritative sources, such as ASPEN units) for each field in that snapshot.	E CRF 827				
F	2	Allow only the authoritative source to update a snapshot data field, with the following exception: • A “super user” can update any field. An audit trail should be maintained to record super user updates.	E CRF 827				
F	3	Validate the sender’s identity through some industry-standard means (account ID, IP address, password, security keys, . . .).	E CRF 827				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	4	Reject updates attempted by any system other than the authoritative source or a super user with a code explaining why. The rejection transaction should be returned to the sender in a timely fashion. The rejection should be logged for the snapshot system administrator to review.	E CRF 827				
F	**4.2.4**	Use CAPRI (or equivalent) for compliance reviews.	L1				
F	1	Report interstate compliance reviews to MCMIS via SAFETYNET	L1				
N	**4.2.5**	Collect, store, analyze, and distribute citation data electronically.	E				Distribute to who – why – citation data is not adjudication data.
F	1	Report citations for interstate operators to MCMIS via SAFETYNET	E				
P	**4.2.6**	Collect, store, analyze, and distribute crash data electronically.	E				Not a means of fully analyzing it currently.
F	1	Report interstate crashes as required to MCMIS via SAFETYNET	E				
P	**4.2.7**	Compute carrier safety risk rating for intrastate carriers based on safety data collected.	E				Working on a system for intrastate at the current time, but don't know when it will be implemented.
P	**4.2.8**	Identify high risk drivers based in the state through regular performance evaluation of various factors such as license status, points, and inspections.	C				Intrastate?

4.3 State CV Administration Systems Design Requirements

The state CV administrative systems are likely to consist of:

- Interstate & Intrastate Vehicle Registration
- Fuel Tax Credentialing/Tax Return Processing
- Credentialing Interface
- Web Site (CRF 1084)
- Carrier Registration (SSRS)
- Driver licensing
- Titling
- Treasury or Revenue
- HazMat Credentialing/Permitting
- Oversize/Overweight Permitting
- Electronic Screening Enrollment – see section 4.4 on Electronic Screening (CRF 1172)

These systems operate at one or more (generally) fixed locations within a state. The systems perform administrative functions supporting credentials and tax regulations. States may form regional alliances to support these functions. Each state coordinates with other states, regional alliances, and CVISN Core Infrastructure systems to support nationwide access to credentials information for administrative and enforcement functions.

When building a credentialing system, it is useful to think about the process of electronic screening enrollment as part of the design criteria. The requirements for Electronic Screening Enrollment have been moved to the section on Electronic Screening, since the enrollment would not occur unless operators wanted to participate in electronic screening. CRF 1172 authorized this change.

CRF 1048 authorized updating CVISN documents to reflect FMCSA's new policy on credentials administration. The policy change resulted from analyzing the results of a survey about electronic credentialing interactions between motor carriers and state information systems (see Reference 38). The new policy is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.
- FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.
- FMCSA encourages the exploration of XML as an alternative to EDI.

This is a policy regarding CVISN Level 1. If a state chooses to implement only a person-to-computer credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state chooses to implement only a computer-to-computer credentialing approach, then implementation of a person-to-computer interface is considered an Enhanced capability. The tables in this section have been updated accordingly.

The concepts in the following table are based on an interpretation of the guiding principles and the state of existing and emerging technologies today. The elements in this table were originally based on the Key Operational Concepts sections of the OCD [Reference 9]. Updated versions of the operational concepts are included in the CVISN Guide to Top-Level Design [Reference 13] and in the CVISN Guide to Credentials Administration [Reference 15]. This version of the COACH reflects the updated concepts.

Table 0-5 CV Administration Operational Concepts

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	1.	Credential applications and fuel tax returns are filed electronically from CVO stakeholder facilities.	L1	
F	2.	Internal state administrative processes are supported through electronic exchange of application data, safety records, carrier background data, and other government-held records.	L1	
F	3.	IRP and IFTA base state agreements are supported electronically.	L1	
F	4.	Credential and fuel tax payment status information for interstate operators are made available electronically nationally to qualified stakeholders.	L1	
F	5.	User access to data is controlled (restricted and/or monitored) where necessary.	L1	Mandatory.
F	6.	Mechanisms are made available for operators to dispute credentials records held by government systems.	L1	
F	7.	Fees and taxes are paid electronically.	E	
N	8.	Electronic access to administrative processes and information is available from "one stop shops" in public sites.	E	Means PCs at counters. Either from the carrier or carrier agents.
F or P	9.	Credential and fuel tax payment status information for intrastate operators are made available electronically to qualified stakeholders throughout the state.	E	

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	10.	Carrier audits are accomplished with electronic support.	C	
F	11.	The "paperless vehicle" concept is supported, i.e. electronic records become primary and paper records become secondary.	C	

The top-level requirements in the following table apply to the design of state credentials-related systems. The table shows more detail about what "CVISN Level 1" means. The CVISN Level 1 requirements are marked with "L1" in the fourth column (Req Level (L1/E/C)). For an overview of CVISN Level 1, see the Introductory Guide to CVISN [Reference 12].

Table 0-6 State CV Administration Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.3.1**	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IRP.	L1 CRF 1048				But not for new licenses.
F	1	Provide a Web site for a person-to-computer process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.
F	2	Provide a computer-to-computer automated process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	2a	Use EDI standards to provide a computer-to-computer automated process.	L1; E CRF 1048				EDI is recommended in the near term for computer-to-computer interfaces.
P	2b	Use XML standards to provide a computer-to-computer automated process.	E CRF 1048				Need to see carrier acceptance of this, else we'll support two system-to-system methods.
F	**4.3.2**	Proactively provide updates to vehicle snapshots as needed when IRP credentials actions are taken.	L1 CRF 1048, 1164				
F	1	Interface to SAFER for interstate vehicle snapshots, using available SAFER interface.	L1 CRF 1048, 1164				Today, EDI is available; plans are to also provide an XML option.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.3.3**	Proactively provide updates to carrier snapshots as needed when IRP credentials actions are taken.	L1 CRF 1048, 1164				
F	1	Interface to SAFER for interstate carrier snapshots, using available standards	L1 CRF 1048, 1164				Today, EDI is available; plans are to also provide an XML option.
F	**4.3.4**	Provide IRP Clearinghouse with IRP credential application information (recaps).	L1				CRF 313 was disapproved; there are no plans for an EDI interface with the IRP CH. The IRP CH interface is specified in IRP CH documents.
F	**4.3.5**	Review fees billed and/or collected by a jurisdiction and the portion due other jurisdictions (transmittals) as provided by the IRP Clearinghouse.	L1				CRF 313 was disapproved; there are no plans for an EDI interface with the IRP CH. The IRP CH interface is specified in IRP CH documents.
F	**4.3.6**	Support electronic state-to-state fee payments via IRP Clearinghouse	L1				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.3.7**	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IFTA registration.	L1 CRF 1048				But not for new licenses and no amended transactions when under audit.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	1	Provide a Web site for a person-to-computer process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.
F	2	Provide a computer-to-computer automated process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.
F	2a	Use EDI standards to provide a computer-to-computer automated process.	L1; E CRF 1048				EDI is recommended in the near term for computer-to-computer interfaces.
P	2b	Use XML standards to provide a computer-to-computer automated process.	E CRF 1048				
F	**4.3.8**	Proactively provide updates to carrier snapshots as needed when IFTA credentials actions are taken or tax payments are made.	L1 CRF 1048, 1164				
F	1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface.	L1 CRF 1048, 1164				Today, EDI is available; plans are to also provide an XML option.
F	**4.3.9**	Provide IFTA Clearinghouse with IFTA credential application information using EDI standards.	L1				
F	**4.3.10**	Support electronic tax filing for IFTA quarterly fuel tax returns.	L1				Quarterly and annual fuel tax returns.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	1	Provide a Web site for a person-to-computer process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.
F	2	Provide a computer-to-computer automated process.	L1; E CRF 1048				Note: Either Web or computer-to-computer interface is required for L1.
F	2a	Use EDI standards to provide a computer-to-computer automated process.	L1; E CRF 1048				EDI is recommended in the near term for computer-to-computer interfaces.
P	2b	Use XML standards to provide a computer-to-computer automated process.	E CRF 1048				
F	**4.3.11**	Provide information on taxes collected by own jurisdiction and the portion due other jurisdictions (transmittals) to the IFTA Clearinghouse using EDI standards.	L1				
F	**4.3.12**	Download for automated review the demographic information from the IFTA Clearinghouse using EDI standards.	L1				
F	**4.3.13**	Download for automated review the transmittal information from the IFTA Clearinghouse using EDI standards.	L1				
F	**4.3.14**	Retrieve IFTA tax rate information electronically from IFTA, Inc.	L1				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.3.15**	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for other credentials.	E				
F	1	Interstate carrier registration	E				
F	2	Intrastate carrier registration	E				
	3	Vehicle title	E				
	4	Intrastate vehicle registration	E				
N	5	HazMat credentialing/permitting, if such credentials/permits are required by state law.	E				
F	6	Oversize/overweight permitting.	E				
	4.3.16	Proactively provide updates to vehicle snapshots as needed when credentials actions are taken.	E				
	1	Vehicle title	E				
	2	Intrastate vehicle registration	E				
F	3	Oversize/overweight permitting.	E				
	4.3.17	Proactively provide updates to carrier snapshots as needed when credentials actions are taken.	E				
F	1	Interstate carrier registration	E				
?	2	Intrastate carrier registration	E				
N	3	HazMat credentialing/permitting, if such credentials/permits are required by state law.	E				
F	4	Oversize/overweight permitting.	E				

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.3.18**	Allow CV operators, government-operated, or third party systems to submit one or more applications in a single transaction.	E				
F	**4.3.19**	Provide commercial driver information to other jurisdictions via CDLIS.	L1				
	4.3.20	Evaluate carrier safety performance prior to issuing vehicle registration renewal (i.e. support PRISM processes or equivalent).	E				
	4.3.21	Allow carriers to provide information for audits electronically.	C				
	4.3.22	Provide titling information to other jurisdictions via NMVTIS.	C				
	4.3.23	Provide revoked IFTA motor carrier information to other jurisdictions via STOLEN.	C				
	4.3.24	Accept electronic credential and supporting electronic documentation, in lieu of paper versions.	C				
	4.3.25	Proactively provide updates to driver snapshots as needed when credentials actions are taken.	C				
	1	Interface to SAFER for driver snapshots, using available SAFER interface.	C				

4.4 State Electronic Screening Systems Design Requirements

The roadside systems involved in electronic screening consist of:

- Screening System
- Roadside Operations System
- Sensor/Driver Communications System
- Electronic Screening Enrollment (CRF 1172)

These electronic screening systems will operate at each fixed or mobile CV check station within a state. The systems perform roadside functions supporting automated carrier, vehicle, and driver identification and associated look-ups in infrastructure-supplied data for credentials and safety checks.

When building an electronic screening system, it is useful to think about the process of electronic screening enrollment as part of the process. The requirements for Electronic Screening Enrollment (ESE) appear in this section on Electronic Screening, since the enrollment would not occur unless operators wanted to participate in electronic screening. CRF 1172 authorized this change. The requirements for ESE should be considered during design of other administrative and credentialing systems.

The concepts in the following table are based on an interpretation of the guiding principles and the state of existing and emerging technologies today. The elements in this table were originally based on the Key Operational Concepts sections of the OCD [Reference 9]. Updated versions of the operational concepts are included in the CVISN Guide to Top-Level Design [Reference 13] and in the CVISN Guide to and Electronic Screening [Reference 16]. This version of the COACH reflects the updated concepts.

Table 0-7 Electronic Screening Operational Concepts

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
F	1.	Widespread participation in electronic screening programs is encouraged.	L1	
F	2.	Jurisdictions disclose practices related to electronic screening.	L1	

Commit Level (F/P/N)	Ite m #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Comments
P	3.	Electronic screening is provided for vehicles equipped with FHWA-specified DSRC transponders. See Reference 35.	L1	Not at all fixed sites – not at mobile sites.
F	4.	Jurisdictions and/or e-screening programs provide a single point of contact for motor carriers to request enrollment in all jurisdictions' electronic screening programs.	L1 CRF 1172	
P	5.	If one jurisdiction or e-screening program provides a transponder to a carrier, it allows the carrier to use that transponder in other jurisdictions' e-screening programs, and in other applications such as electronic toll collection.	L1 CRF 1172	
P	6.	For an enrolled carrier that has vehicles equipped with compatible transponders, jurisdictions and/or e-screening programs provide a mechanism for participation in electronic screening using those transponders.	L1 CRF 1172	Depends on interoperability & requirements.
F	7.	Credentials and safety checks are conducted as part of the screening process.	L1	
P	8.	Fixed and/or mobile roadside check stations are employed for electronic clearance functions, according to the jurisdiction's needs and resources.	L1	Probably not mobile. Not all fixed.
P	9.	Jurisdictions support a common set of screening criteria.	E	What if states want to have additional criteria?
P	10.	Screening systems are interoperable with those in different jurisdictions.	E	Depends what other have?

The top-level requirements in the following table apply to the design of state screening-related systems. The table shows more detail about what "CVISN Level 1" means. The CVISN Level 1 requirements are marked with "L1" in the fourth column (Req Level (L1/E/C)). For an overview of CVISN Level 1, see the Introductory Guide to CVISN [Reference 12].

Table 0-8 State Electronic Screening Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	**4.4.1**	Follow FHWA guidelines for Dedicated Short Range Communications (DSRC) equipment.	L1 CRF 1159				See the NPRM regarding DSRC in ITS CVO, Reference 35.
F	1	For the immediate future, all CVO and Border crossing projects will continue to utilize the current DSRC configuration employed by the programs. This is the "ASTM version 6" active tag.	L1 CRF 1159				The DSRC provisional standard is defined in the FHWA specification, (Reference 37).
	2	Beginning January 1, 2001, all CVO and Border Crossing projects will use a provisional standard as described below. In addition, this provisional standard will be designed to ensure interoperability with the existing legacy equipment used in CVO that conforms to ASTM Version 6.	E CRF 1159				
	2a	the new ASTM Physical Layer in the active mode;	E CRF 1159				Reference 32.
	2b	the existing ASTM Version 6 Data Link layer in the synchronous mode;	E CRF 1159				Reference 33.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
	2c	and the IEEE 1455 Application Layer.	E CRF 1159				Reference 34.
F	**4.4.2**	Use snapshots updated by a SAFER/CVIEW subscription in an automated process to support screening decisions.	L1 CRF 1171				
F	1	Carrier snapshots.	L1				
F	2	Vehicle snapshots.	L1				
F	3	Driver snapshots.	C				Will have the data, don't know if it will be used.
F	**4.4.3**	Implement interoperability policies as they are developed by ITS America, the American Association of State Highway Transportation Officials, HELP, Inc., MAPS, Advantage CVO, I-95 Corridor Coalition, and the Commercial Vehicle Safety Alliance.	L1				
F	1	See AASHTO's Commercial Vehicle Electronic Screening Interoperability Policy Resolution, PR-14-97, Reference 20.	L1				
F	**4.4.4**	Provide electronic mainline or ramp screening for transponder-equipped vehicles, and clear for bypass if carrier & vehicle were properly identified and screening criteria were passed.	L1				Not all sites – not mobile operations.
F	1	For transponder-equipped vehicles, identify carrier at mainline or ramp speeds.	L1				Not all sites – not mobile operations.

Commit Level (F/P/N)	Item #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Date	IOC Date	FOC Date	Comments
F	2	For transponder-equipped vehicles, identify vehicle at mainline or ramp speeds.	L1				Not all sites – not mobile operations.
F	3	Use WIM or weight history at mainline speed or on the ramp in making screening decisions.	L1				Not all sites – not mobile operations.
F	4	Record screening event data.	E				
N	5	For transponder-equipped vehicles, identify driver at mainline or ramp speeds.	C				Not included at this time.
F	**4.4.5**	Collect from the carrier a list of jurisdictions and/or e-screening programs in which it wishes to participate in electronic screening and inform those jurisdictions and/or e-screening programs.	L1 CRF 1172				
F	**4.4.6**	Collect from the carrier a list of jurisdictions and/or e-screening programs in which each of its vehicles chooses to participate in e-screening, and inform those jurisdictions and/or e-screening programs.	L1 CRF 1172				
F	**4.4.7**	Record transponder number and default carrier ID for each vehicle that intends to participate in e-screening	L1 CRF 1172				
F	**4.4.8**	Share carrier ID for each carrier that intends to participate in e-screening with other jurisdictions and/or e-screening programs as requested by the carrier.	L1 CRF 1172				

Com mit Level (F/P/ N)	Ite m #	Compatibility Criteria	Req Level (L1/E/C) CRF #	Op Test Dat e	IOC Dat e	FO C Dat e	Comments
F	1	Via SAFER snapshots	E CRF 1172				
F	**4.4.9**	Share transponder number and default carrier ID for each vehicle that intends to participate in e-screening with other jurisdictions, e-screening programs, or other agencies as requested by the carrier.	L1 CRF 1172				
F	1	Via SAFER snapshots	E CRF 1172				
F	**4.4.10**	Accept each qualified vehicle already equipped with a compatible transponder into your e-screening program without requiring an additional transponder.	L1 CRF 1172				
F	**4.4.11**	Enable the carrier to share information about the transponder that you issue with other jurisdictions, e-screening programs, or agencies.	L1 CRF 1172				
F	**4.4.12**	Verify credentials/safety information with authoritative source prior to issuing citation.	L1				As possible.
F	**4.4.13**	If a vehicle illegally bypasses or leaves the CV check station, alert law enforcement for possible apprehension.	C				
	4.4.14	Report periodically to State safety information system on the activities conducted at each station (e.g. statistics).	C				Who is the State safety information entity?

5. References

1. JHU/APL, *ITS/CVO CVISN Glossary*, POR-96-6997 V1.0, dated December 1998.

2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists, SSD/PL-97-0236, POR-97-7067 P 1.0, Commercial Vehicle Information Systems and Networks (CVISN) Operational and Architectural Compatibility Handbook (COACH),* dated March 1997. The latest version is available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/]

3. JHU/APL, *Updates to COACH Part 1: Chapter 5 (State), Chapter 6 (CVISN Core Infrastructure), and Chapter 7 (Carrier)*, SSD/PL-98-0017, dated January 1998.

4. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 - Project Management Checklists, POR-97-7067 P2.0, (Preliminary Version),* September 1999. The latest version is available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

5. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists, POR-97-7067 P1.0,* May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

6. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists, POR-97-7067 D1.0, (Draft)*, April 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

7. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 - Interoperability Test Criteria, SSD/PL-99-0470, (Draft), dated July 1999*. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

8. JHU/APL, *Introduction to Commercial Vehicle Information Systems and Networks (CVISN)*, POR-95-6982, V1.0, March 14, 1997.

9. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Operational Concept Document*, (Preliminary Issue P.2), POR-96-6989, June 1996.

10. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Architecture Specification*, (Preliminary), POR-96-6985, February 1996.

11. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V1.0, (Baseline Version), March 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
12. JHU/APL, *Introductory Guide to CVISN, POR-99-7186 P.1 (Preliminary),* May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
13. JHU/APL, *CVISN Guide to Top-Level Design, POR-99-7187, P.1*, May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
14. JHU/APL, *CVISN Guide to Safety Information Exchange, POR-99-7191, D.1*, March 2000. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
15. JHU/APL, *CVISN Guide to Credentials Administration, POR-99-7192, P.1*, July 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
16. JHU/APL, *CVISN Guide to Electronic Screening, POR-99-7193, D.1*, October 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]
17. Intelligent Transportation Society of America, *ITS CVO Guiding Principles*, published on the World Wide Web at http://www.itsa.org, last updated March 27, 1998.
18. Intelligent Transportation Society of America, *Fair Information Principles for ITS/CVO*, published on the World Wide Web at http://www.itsa.org, last updated January 12, 1999.
19. Intelligent Transportation Society of America, *Interim ITS/CVO Interoperability Guiding Principles*, published on the World Wide Web at http://www.itsa.org, last updated January 12, 1999.
20. AASHTO (American Association of State Highway Transportation Officials), *Policy Resolution P$-14-97 Commercial Vehicle Electronic Screening Interoperability, AASHTO Transportation Policy Book*, January 1999. The document is available on the World Wide Web at http://www.aashto.org/.
21. FHWA, *Commercial Vehicle Information Systems and Networks (CVISN) Model Deployment Program Request for Information*, notice in Federal Register April 11, 1996 (volume 61, number 71, 16157)
22. FHWA, *Commercial Vehicle Information Systems and Networks (CVISN) Model Deployment Program Request for Application*, notice in Federal Register July 5, 1996 (volume 61, number 130, 35300).

23. FHWA, Letter from HAS-20 to States, *Call for New CVISN States - What states are interested in CVISN Workshops*, J. Loftus e-mail dtg 981222 5:10 PM

24. Reference Deleted

25. ANSI ASC X12, *Electronic Data Interchange X12 Standards*, Draft Version 4, Release 3, (a.k.a. Release 4030), December 1999.

26. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Recommendations for Common Carrier, Vehicle, Driver, and Cargo Identifiers*, SSD/PL-99-0388, June 1999.

27. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume I - IRP Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-96-6993 D.5, dated March 2000.

28. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume II – IRP Interstate Credential Transactions*, Draft Version, POR-96-6994 D.2, December 17, 1996.

29. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume III - International Fuel Tax Agreement (IFTA) Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-97-6996 D.4, dated March 2000.

30. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume IV - Oversize / Overweight (OS/OW) Credential Transactions*, POR-97-7068 D.3, dated March 2000.

31. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Safety and Credentials Information Exchange (Transaction Set 285)*, POR-96-6995 D.5, dated March 2000.

32. ASTM Preliminary Standard-111-98, Specification for Dedicated Short Range Communication (DSRC) Physical Layer using Microwave in the 920 to 928 MHz band, dated April 1999. For a summary of the standard, see http://www.its.dot.gov/standard/standard.htm.

33. ASTM Draft Standard for Dedicated, Short Range, Two-Way Vehicle to Roadside Communications Equipment, Draft 6, dated 23 February 1996.

34. IEEE Standard 1455-99, Standard for Message Sets for Vehicle/Roadside Communications, dated September 1999. For a summary of the standard, see http://www.its.dot.gov/standard/standard.htm.

35. The U. S. Department of Transportation, Federal Highway Administration, *Proposed Rule: Dedicated Short Range Communications In Intelligent Transportation Systems (ITS) Commercial Vehicle Operations*, 23 CFR Part 945, [FHWA Docket No. FHWA 99-5844] RIN 2125-AE63, published in Federal Register: December 30, 1999 (Volume 64, Number 250)], Page

73674-73742. Available from the Federal Register Online via GPO Access, http://www.access.gpo.gov/su_docs/aces/aces140.html [DOCID:fr30de99-43]

36. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists, SSD/PL-97-0243, POR-97-7067 V1.0, Commercial Vehicle Information Systems and Networks (CVISN) Operational and Architectural Compatibility Handbook (COACH)*, dated March 1999.

37. JHU/APL, *Delivery of Draft Specification for "Active Sandwich" Protocol for Dedicated Short Range Communications (DSRC) for Commercial Vehicles, SSD-PL-99-0784, with enclosure Draft Specification for DSRC for Commercial Vehicles, Version 0.0.1, November 1999*, dated December 1999.

38. JHU/APL, *Delivery of CVISN Electronic Credentialing Preference Survey Results, SSD-PL-00-0408, with enclosure Electronic Credentialing Preference Survey Results*, June 2000, dated July 2000.

Appendix B – COACH Part 2

Intelligent Transportation Systems (ITS)

Commercial Vehicle Operations (CVO)

CVISN Operational and Architectural Compatibility Handbook (COACH)

Part 2

Management Checklists

Preliminary Version

POR-97-7067 P2.0

Program / Project Management Checklist

This section defines the overall program and project management practices which are recommended for every CVISN state.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	1. Establish program executive sponsorship. For example an agency head or chief information officer; or a group such as an executive-level steering committee.	
F/P	2. Empower a Program Manager, dedicated to the program at least 30% of the time on average. More time is needed in the startup phase, when a team is new, and if there are many simultaneous projects under the CVISN umbrella. (One state with 20 projects has a full-time Program Manager.)	The time may be split among 2 people.
F/P	3. Engage a System Architect, dedicated to the program approximately 80% of the time on average.	Depends upon funding.
F/P	4. Engage a facilitator/scheduler/administrator, dedicated to the program approximately 50% of the time on average.	Depends on funds & % may be lower.
F	5. When multiple state agencies are involved, establish an inter-agency coordinating council.	
F	6. Obtain an approved memorandum of agreement among all involved state agencies.	Statement of Work.
F	7. Establish a state carrier advisory council.	Wisconsin already has a Motor Carrier Advisory Committee.
F	8. Recruit interstate, intrastate, and owner-operator carriers to participate in the program before production deployment (both motor carriers and motor coach companies).	Wisconsin already does this.
F	9. Where appropriate initiate separate deployment projects under the scope of the CVISN program. For example, deployments in disparate domains such as credentials administration vs electronic screening are likely to be developed by different teams operating as distinct projects.	Separate projects will be initiated by both State Patrol and Motor Vehicle Redesign units.
F	10. Assign a Project Leader for each separate deployment project, dedicated to each project at least 30% of the time on average. More time is needed in the startup phase.,	This is standard project development policy. The % may be less.
F	11. Provide adequate training opportunities to project team members, such as attendance at FHWA's CVISN training courses and CVISN workshops.	Not all team members of each project will attend these workshops.
F	12. Ensure all team members acquire a broad and common understanding of CVISN activities, architecture, and design guidance -- for example, by reading the CVISN Guides, and noting lessons-learned by other states.	
F	13. Foster a sense of professional fellowship and teamwork. Likely to require teambuilding interventions such as a partnering workshop; and periodic face-to-face meetings of geographically dispersed teams.	This is standard project development policy.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	14. Adopt the strategy of incrementally developing and deploying products in 3-6 month phases, where each phase adds additional CVISN capabilities. This is called the "spiral" development model as opposed to the "linear" model. Refer to the CVISN Guide to Phase Planning & Tracking.	This approach is already being used in the OSOW area, and will be continued for future CVISN projects.
F	15. Establish a configuration management process for controlling changes to the system baseline; this typically includes a Configuration Control Board. Utilize state's existing configuration control process wherever possible.	Standard project development policy includes configuration management control.
F	16. Set up a program library; obtain needed references identified in the CVISN Guide to Program & Project Planning.	Repository established by J. Anderson.
F	17. Maintain a list of action items, decisions, and issues. (By definition action items require formal closure.)	BAS will maintain a standard "issues" list for project-related action items, decisions, and issues. The program side will probably keep a separate list of program-related issues.
F	18. Delineate needs for external communications with stakeholders (including the state legislature), and with related projects.	Communication needs with both internal and external stakeholders are identified for each project within the project proposal document.
F	19. Conduct monthly team meetings and status assessments.	At the project level, weekly meetings are held with project leaders for status assessment. Individual team meetings are held as needed.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	20. Track progress versus schedule monthly; strategize accordingly.	Projects are tracked visually through several monitoring tools, including reports that are reviewed with the executive sponsors (DMV Directors)
F	21. Conduct quarterly stakeholder progress reviews before a wider audience.	Monthly DMV Directors and CVISN Steering committee reviews already occur. MCAC meets 3 times a year.
F	22. Monitor actual costs and resource expenditures relative to estimates.	This is standard project development policy.

Program / Project Planning Checklist

This section defines desired elements of the CVISN program plan, and the subsidiary project plans. It also defines the recommended approach.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	1. Review state's ITS/CVO strategic plan and business plan.	This documentation will be important basic information for Project Leaders and team members. Program-side participants will also most likely use this information to become familiar with the overall direction.
F	2. Define objectives for CVISN Program.	This is already taking place with the CVISN core team, composed of IT and program resources.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	3. Derive requirements for deployment projects.	BAS will probably lead the effort to identify requirements for each project, with full participation and input from the program side.
F	4. Establish project development standards, such as design margin as a function of development lifecycle.	Standards and guidelines for project development will be used.
F	5. Define project-specific processes, such as required design reviews, or how to close an action item.	These are part of the standards and guidelines for project development.
F	6. Establish a system design baseline. (See the CVISN Guide to Top-Level Design.)	Assume this will be done, probably by the Project Manager/team.
F	7. Create a program Work Breakdown Structure.	Assume this will be done as part of the Program planning effort. As part of each project, a WS will be produced as part of the project proposal.
F	8. Delineate program deliverables, including support documentation and training.	These are part of the standards and guidelines for project development, and are identified in the project proposal.
F	9. Establish a program organization structure, with clear roles and responsibilities.	Assume this will be done at the program level, and it will also be done individually as part of the proposal for each project.
F	10. Assign each element of the work breakdown structure to an element of the program organization structure.	Standard project development policy at the project level.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	11. Develop project-specific "partnering charters" covering four areas: mission statement; communication objectives (e.g. decision-making at lowest possible level); performance objectives (e.g. complete the project without litigation); issue resolution system (e.g. management levels and timeframes).	Each project will have a separate proposal that will outline the mission, goals and objectives for communication, performance, and issue resolution among other things.
F	12. Develop a flexible procurement strategy. Allocate sufficient calendar time for the required steps.	Procurement procedures are in place and flexible enough to meet the needs of this project.
F	13. Establish a top-level schedule divided into phases; ensure milestones are measurable.	This is typically done as part of the initial proposal for a multi-phase project, and is revisited as each phase completes and a new one starts.
F	14. Outline high-level objectives for each phase; express in a 1-2 page phases chart that explains capabilities from a user's point of view.	This is typically done as part of the initial proposal for a multi-phase project, and is revisited as each phase completes and a new one starts.
F	15. Set the stage for the transition to production use and support; such as database backup and restoration, and a user "help" desk.	Standard project development policy.
F	16. Identify project external dependencies, with their need-by date.	Standard project development policy.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	17. Estimate cost and resource requirements first using summary top-down methods, such as historical analogy and manager's judgment. This will initiate the process and set targets.	This is usually done as part of the 'abstract' process, which seeks to establish initial cost targets. It is later revised with a bottom-up approach in the proposal.
F	18. Estimate cost and resource requirements using bottoms -up detailed methods, such as resource-type quantities for each element of the WBS. This will get 'buy in" from the staff, and validate the top-down estimates.	Done as part of the proposal process.
F	19. Determine potential funding sources and obtain funding commitments	Standard project development policy.
F	20. Identify both programmatic and technical issues and develop a resolution plan.	Standard project development policy.
F	21. Obtain approval, publish, and distribute program plan document. Include completed COACH Part 2 checklists as an appendix.	Assume the program plan will follow the same procedures for development and publication as the project proposals.
F	22. Maintain on each project a Project Leader's notebook with up-to-date copies of essential key charts and diagrams.	This information, along with other important documentation, notes, and data becomes the "Project File" upon completion of the project, and is kept for later lookup and reference.
F	23. Maintain a Program Manager's notebook with up-to-date copies of essential key charts and diagrams.	Assume this will be done by the Program Manager, similar to what Project Leaders will do.
F	24. Once a year or more often, re-figure the estimate-to-completion.	Standard project development policy for multi-phase projects.

Phase Planning and Incremental Development Checklist

This section defines desired elements of the CVISN phase plan, and the recommended method of approach for phase planning and incremental development. Phase planning is performed for each project, and aggregated for the CVISN program. Incremental development is project-specific but applied program-wide. Incremental deployment is the outcome of incremental development.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	1. Sustain a system perspective -- a vision of the overall CVISN architecture and deployment strategy.	Assuming funding is available to embark on this effort, the vision established through the CVISN Business Plan and developed more fully in the CVISN Level 1 Planning Process will be followed through in planned projects.
F	2. Plan, develop, and release incrementally, such that at the end of each phase useful end-to-end functionality is delivered in a way that subsequent phases can build upon.	Standard project development policy.
F	3. Choose and format the elements of the phase plan such that they are naturally useful for presenting status. For example, the list of deliverables could also include columns for dates, current standing, and reasons for change.	Phase plans are included as part of the Proposal at the start of each phase, and include elements useful for status reporting.
F	4. Employ the rolling wave planning technique, with more detail for the near-term tasks and progressively less detail for the far-term tasks.	This is done with the initial Proposal, and revised prior to the start of each new phase.
F	5. Involve the project staff in the phase planning process, for example in a team-oriented planning session.	Standard project development policy.
F	6. Review items on the issues list; resolve to the extent possible.	Standard project development policy.
F	7. Close open action items, to the extent possible.	Standard project development policy.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	8. Review items on the decisions list -- as a reminder and to verify they are still relevant and correct.	Standard project development policy.
F	9. Set phase objectives.	Done as part of the proposal for each specific phase.
F	10. Flesh out the applicable lowest-level details of the Work Breakdown Structure.	Done as part of the proposal for each specific phase.
F	11. Derive phase requirements; refer to COACH Part 1 checklists and the Program Plan as starting points. Look for alternative design and development approaches.	Done as part of the proposal for each specific phase.
F	12. Itemize phase deliverables.	Done as part of the proposal for each specific phase.
F	13. Indicate which elements of the system design baseline are to be deployed; update presentation diagrams accordingly.	Done as part of the proposal for each specific phase.
F	14. Perform studies to determine whether to make, buy, or modify subsystem components.	Standard project development policy.
F	15. Develop a detailed schedule for the work to be accomplished during the current phase. Most effectively done by identifying and linking activities per the critical path method, utilizing a desktop scheduling tool. The output can be printed as both a Gantt (bar) chart and a PERT (network) chart.	Standard project development policy.
F	16. Identify named individuals who will perform the activities in the detailed schedule.	Standard project development policy.
F	17. Update project external dependencies, with their need-by date.	Standard project development policy.
F	18. Update the master program phases chart.	This would probably be presented in the proposal for the current phase, and as such would be the most up-to-date version of the planned phases.

Commit (F/P/N)	Intended Actions	Preparer Comments
F	19. Complete the detailed design for all components and interfaces to be developed or modified in the phase. Start with the top-level design and phase objectives. Use COACH Part 3 checklists as guidance, plus the Scope and Design Workshops.	Standard project development policy.
F	20. Define subsystem and component control and data interfaces. Utilize COACH Part 4 for functional allocation.	Standard project development policy.
F	21. Conduct technical reviews in order to catch problems as early as possible in the development life cycle.	Standard project development policy.
P/F	22. Maintain a strict version numbering system for all products.	Not a standard element of our development process, but it could be implemented if necessary.
F	23. Maintain stakeholder commitment via visibility into progress by physical demonstrations of useful capability, and by regular management status reporting.	Standard project development policy.
F	24. Define system acceptance criteria; use COACH Part 5 checklists as guidance.	Standard project development policy.
F	25. Conduct operational acceptance tests at the end of each phase; specify re-work if necessary.	Standard project development policy.
P/F	26. Conduct a lessons learned session at the end of each phase (as part of planning the next phase).	Not always done for each project, but where appropriate it can be conducted.

References

1. **CVISN Website** hosted by the Johns Hopkins University Applied Physics Laboratory (JHU/APL) at http://www.jhuapl.edu/cvisn/.

2. JHU/APL, ***CVISN Toolkit CD ROM***. *A comprehensive set of technical documentation and planning tools assembled on a CD-ROM to assist new CVISN deployment states in the development of their CVISN Project Plans before, during, and after the CVISN Workshops.*

3. JHU/APL, ***ITS/CVO CVISN Glossary***, POR-96-6997. Available on-line at the CVISN Website [1].

4. JHU/APL, ***CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists***, POR-97-7067. Available on-line at the CVISN Website [1].

5. JHU/APL, ***CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists***, POR-97-7067. Available on-line at the CVISN Website [1].

6. JHU/APL, ***CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists***, POR-97-7067. Available on-line at the CVISN Website [1].

7. JHU/APL, **CVISN Operational and Architectural Compatibility Handbook (COACH), Part *5 - Interoperability Test Criteria***, POR-98-7126. Available on-line at the CVISN Website [1].

8. JHU/APL, ***Introductory Guide to CVISN***, POR-99-7186. Available on-line at the CVISN Website [1].

9. JHU/APL, ***CVISN Guide to Program & Project Planning***, POR-99-7188. *Appendix A lists valuable project management references, including quite a few that published "lessons learned" from ITS deployments throughout the country*. Available on-line at the CVISN Website [1].

10. JHU/APL, ***CVISN Guide to Phase Planning & Tracking***, POR-99-7189. Available on-line at the CVISN Website [1].

11. JHU/APL, ***CVISN Guide to Top-Level Design***, POR-99-7187. Available on-line at the CVISN Website [1].

12. JHU/APL, ***CVISN Guide to Integration and Test***, POR-99-7194. Available on-line at the CVISN Website [1].

13. JHU/APL, ***CVISN Guide to Safety Information Exchange***, POR-99-7191. Available on-line at the CVISN Website [1].

14. JHU/APL, ***CVISN Guide to Credentials Administration***, POR-99-7192. Available on-line at the CVISN Website [1].

15. JHU/APL, ***CVISN Guide to Electronic Screening***, POR-99-7193. Available on-line at the CVISN Website [1].

Appendix C – COACH Part 3

Intelligent Transportation Systems (ITS)

Commercial Vehicle Operations (CVO)

CVISN Operational and Architectural Compatibility Handbook (COACH)

Part 3

Detailed System Checklists

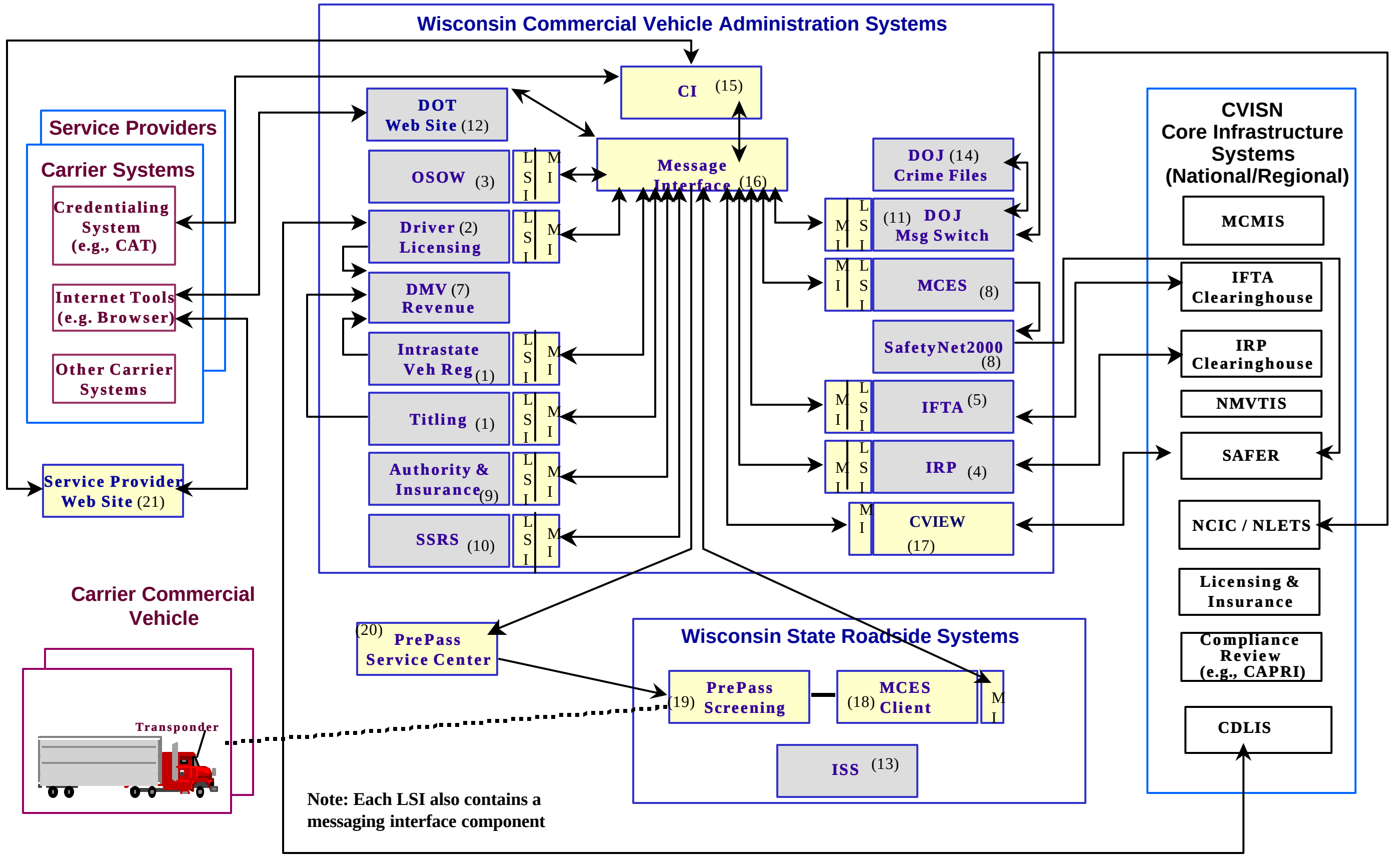
Baseline Version

POR-97-7067 V1.0

October 2000

Wisconsin Top Level Design

4/19/2001



Wisconsin Commercial Vehicle Administration Systems

CI (15)

DOT Web Site (12)

Message Interface (16)

OSOW (3)

Driver (2) Licensing

DMV (7) Revenue

Intrastate Veh Reg (1)

Titling (1)

Authority & Insurance (9)

SSRS (10)

DOJ (14) Crime Files

(11) DOJ Msg Switch

MCES (8)

SafetyNet2000 (8)

IFTA (5)

IRP (4)

CVIEW (17)

LSI

MI

Service Providers

Carrier Systems

Credentialing System (e.g., CAT)

Internet Tools (e.g. Browser)

Other Carrier Systems

Service Provider Web Site (21)

Carrier Commercial Vehicle

Transponder

(20) PrePass Service Center

Wisconsin State Roadside Systems

(19) PrePass Screening

(18) MCES Client

ISS (13)

Note: Each LSI also contains a messaging interface component

CVISN Core Infrastructure Systems (National/Regional)

MCMIS

IFTA Clearinghouse

IRP Clearinghouse

NMVTIS

SAFER

NCIC / NLETS

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Figure 0-1 Wisconsin State Design Template

Data Maintenance Requirements

The checklists in this chapter summarize the requirements for maintaining data and sharing updates with other CVO stakeholders. Systems should be designed to meet these criteria. If a user group has more stringent requirements, those requirements override these and should be noted in the "Comments" column.

In accordance with CRF 1204, this chapter has been updated to provide more guidance to the states. Instructions for how to complete Table 2-1 have been added to this chapter.

The "Commit" column in Table 2-1 should be used to indicate the state's commitment to the data maintenance/update requirement stated in the "Requirement for data to be maintained or updated" column. As in the COACH Part 1, the codes for commitment are defined as:

- Commit Level (F/P/N) – the state's commitment level to the item

  Using the first column of each checklist entry, a **commitment level should be filled in** by the state. There are three possible levels of commitment:

  (F) This rating indicates a full commitment. This level means that at least 80% of the state's systems involved in the process implied by the checklist item are compatible or are intended to be compatible with the checklist item statement.

  (P) This rating indicates a partial commitment. This level means that between 50% and 80% of the state's systems involved in the process implied by the checklist item are compatible or are intended to be compatible with the checklist item statement.

  (N) This rating indicates no commitment. This level means that less than 50% of the state's systems involved in the process implied by the checklist item are compatible or are intended to be compatible with the checklist statement.

If the state maintains its master copy of this document electronically, the following conventions are recommended when filling in the column to illustrate the "firmness" of the state's plan:

- *Italics type* : Tentative, not approved by the final decision makers
- Regular type : Approved by the decision makers (or supported by consensus)
- **Bold type** : Completed

For a state to be "compatible with CVISN," it must implement selected items in Table 2-1. To distinguish those items, the CVISN project team has assigned a **compatibility requirement level** to each checklist item. As in the COACH Part 1, the codes for the "Reqts Level" column are defined as:

(L1) This rating identifies a CVISN Level 1 compatibility requirement.

(E) This rating indicates an enhanced level of CVISN compatibility. These items may require a little longer to complete (3-4 years).

(C) This rating indicates a complete level of CVISN Compatibility. Satisfying all these provides complete CVISN compatibility. These items are expected to require a longer-range (5 or more years) time frame.

States are expected to focus initially on checklist items with an "L1" compatibility requirement level rating. Making a *partial commitment* indicates that the state will at least demonstrate the feasibility of that data maintenance and/or update requirement. Making a *full commitment* indicates that the state will fully implement the data maintenance and/or update requirement and be ready for the next steps.

Table 0-1. Data Maintenance & Update

Commit Level (F/P/N)	Data Need Category	Requirement for data to be maintained or updated	Reqts Level	Comments
F for L1	1. *Routine snapshot segment changes* are those for which users can wait until the next routine snapshot update is scheduled. Routine snapshot data changes include updates related to passed inspections, compliance reviews, or credential renewals or supplements.	The authoritative source system should update the snapshot record within 24 hours of the change.	L1; C	L1 for carrier & vehicle snapshots; C for driver snapshots
F for L1	2. *High-priority snapshot segment changes* are those which users need to know about immediately. High priority snapshot data changes include out-of-service (OOS) resulting from an inspection.	The source system should update the snapshot record within 30 minutes of the change.	L1; C	L1 for carrier & vehicle snapshots; C for driver snapshots
F for L1	3. *Snapshot subscription fulfillment* is the SAFER or CVIEW process for sending specified snapshot output views to users based on standing requests to do so when specified data changes.	Whenever the criteria for sending a snapshot are triggered, the snapshot system (CVIEW or SAFER) should distribute the revised snapshot within 24 hours for routine snapshot segment changes, and within 30 minutes for high-priority snapshot segment changes.	L1; C	L1 for carrier & vehicle snapshots; C for driver snapshots
F	4. *An inspection report* indicates the results of an inspection conducted at the roadside by a qualified inspector.	Normally, the results of an inspection using ASPEN should be reported electronically within 24 hours of being conducted. If the vehicle or driver was placed OOS, the results should be reported within 30 minutes.	L1	

Commit Level (F/P/N)	Data Need Category	Requirement for data to be maintained or updated	Reqts Level	Comments
F	5. *Credential application response* is the response from the state to the applicant. In this context, the "response" reflects the results of evaluating the credential application.	The state system should respond to the applicant's system within 2 hours for a correct transaction that requires no manual intervention. If manual intervention is required, the state system should respond to the applicant's system within 24 hours of receipt of an electronic input.	L1	
F	6. *IRP base state agreement data* are those data required by other jurisdictions to understand the fees collected on their behalf. In IRP lingo, these data are exchanged via "recaps."	The state IRP system should send recaps to the IRP Clearinghouse at least monthly.	L1	
F	7. *IFTA base state agreement data* are those data required by other jurisdictions to understand the quarterly fuel taxes collected on their behalf. In IFTA lingo, these data are called "demographic" for basic census information, and "transmittal" for tax return information.	The state IFTA system should send updated demographic and transmittal data to the IFTA Clearinghouse at least monthly.	L1	
F	8. The *Privacy Act of 1974* [Reference18] attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. Federal systems must adhere to the law. Some sections of the law apply to state and local governments as well. Additionally, some states have related laws regarding privacy and data access.	The systems affected by the Act or related statutes should incorporate procedures, protocols, and designs that support the law. The Privacy Act include sections concerning data disclosure, accounting of disclosure, access, amendment, reporting, archiving, and other activities.	L1	

Description of State Safety Information Exchange and Safety Assurance System Components

Table 3-1 lists the Safety Information Exchange and Safety Assurance products in the generic CVISN state system design. The state should use this checklist to map the state's specific products to the generic components and to reflect the state's specific design.

Table 0-2 State Safety Information Exchange and Safety Assurance System Components

Commit Level (F/P/N)	System Name in Generic Design	System Name in Our State	Differences between Our State and the Generic Functions (+, -, none)	Comments
F	SAFETYNET	SAFETYNET	None	
F	Inspections - ASPEN	MCES	+	
F	Inspections - ISS	ISS	None	
N	Inspections - ISS-2			Possible Future Implementation
F	Inspections - PIQ	MCES	+	
F	CVIEW	CVIEW	+	To Be Built / Bought
F	Citation & Accident	Citation & Accidents	-	Need To Add Snapshots
F	Compliance Review - CAPRI	CAPRI	None	

The paragraphs in this section describe the functions of each Safety Information Exchange and Safety Assurance product in the generic CVISN state system design. In accordance with CRF 1204, several system descriptions were updated using information from Reference 21. The state should modify the paragraphs in this section to reflect its specific component names and functionality.

SAFETYNET

This product was developed and is maintained by FMCSA. SAFETYNET, operating in every state, is used to collect safety data, analyze and edit the data, and report safety data to FMCSA's MCMIS. According to Reference 12, SAFETYNET is the state-level information management system for motor carrier safety. SAFETYNET captures inter- and intra-state driver/vehicle inspection data, accident data, carrier compliance reviews, enforcement data, and carrier identification data. Originally designed as a manual data entry system, SAFETYNET now allows electronic data collection. The system is central to successful management and operation of the Motor Carrier Safety Assistance Program (MCSAP). It contains many report-generating, prioritizing and task tracking routines. SAFETYNET 2000 is an Oracle-based client-server, Structured Query Language (SQL) database management system.

Inspections (e.g. ASPEN, ISS-2, PIQ)

Record & report safety inspections. According to Reference 12, ***ASPEN*** is a driver/vehicle safety inspection software package that improves the entire inspection process by providing inspectors at the roadside access to safety performance information including the most recent inspection results, the driver's CDL status (see CDLIS) and the safety performance and past safety problems of the carrier (see ISS). ASPEN can be seen as an intelligent assistant that ensures complete and accurate data collection at the roadside. Inspectors select applicable violations from lists of possible citations and add descriptive notes as needed. The program can be customized for use by different States. ASPEN prints an inspection report on-site that is given to the driver. A copy also can be faxed to carrier management. ASPEN inspection data is electronically transferred to State information systems via CVIEW and SAFER. Optimized for use with pen-computers, ASPEN can also be run on Mobile Data Terminals and laptop computers. ASPEN's functions include:

- Interface with Roadside Operations system (to get screening data, notify when inspector available)
- Interface with CDLIS to check CDL status
- Interface to CVIEW/Data Mailbox system (directly or via Roadside Ops) to report inspections and access snapshots and safety reports
- Inspect vehicle - provide operator data entry of inspection results
- Update ASPEN internal database
- Calculate/display Inspection Selection System (ISS) value which recommends inspection based on carrier safety history

According to Reference 12, ***ISS*** is a standardized algorithm that uses carrier safety performance and inspection history data to rank carriers according to the relative value of conducting a vehicle inspection. The objective is to increase inspections on carriers with poor safety performance records (accidents, out-of-service defects and other safety problems) while also increasing inspections on carriers where there is little available information. ISS runs within ASPEN and also as a stand alone for Port of Entry use. Eventually it may also be used for mainline vehicle screening.

The ***ISS-2*** algorithm is substantially different from ISS. ISS is based on the Safety Status Measurement System (SafeStat) algorithm; ISS-2 is not. ISS-2 is computed on the same mainframe, located at the Austin Automation Center (AAC), that runs the MCMIS software; ISS scores were computed on individual laptops in the field based on safety data supplied to those units by SAFER via the subscription process. ISS-2 scores are normalized from 1 - 100, whereas the SafeStat range used by ISS is considerably larger. ISS-2 also accounts for carriers lacking sufficient data to compute a score by artificially assigning them a high score, e.g. 100, thus ensuring that vehicles for those carriers are inspected.

PIQ is an information retrieval application that allows federal and state law enforcement personnel to quickly obtain recent past vehicle safety inspections on any vehicle regardless of where the inspection was performed. PIQ executes on roadside desktop, laptop, and pen computers. It links to the SAFER system, via the SAFER Data Mailbox, to query and retrieve past inspections based on power unit plate number and state ID. These "past" inspections are saved in SAFER for a 45 day period. Using PIQ, inspection reports can be queried and retrieved at the roadside within seconds of a user's request.

CVIEW
Commercial Vehicle Information Exchange Window. This product is a spin-off of the FMCSA-developed SAFER system. It is owned by and located in a state. In CVISN Level 1, there is a requirement to implement a system called CVIEW (Commercial Vehicle Information Exchange Window) or its equivalent for snapshot exchange within the state and to other states. The CVIEW or equivalent functions for handling the exchange of safety and credentials information within the state, and with other jurisdictions via SAFER, are listed below:

- Provide for the electronic exchange of:
  - **interstate** carrier and vehicle safety and credential data between state source systems, users, and SAFER
  - **intrastate** carrier and vehicle safety and credential data between state source systems and users
- Serve as the repository for a state-selected subset of

  - **interstate** carrier and vehicle safety and credential data
  - **intrastate** carrier and vehicle safety and credential data
- Support safety inspection data reporting & retrieval by roadside enforcement personnel
- Provide inter- and intrastate carrier and vehicle safety and credential data to the roadside to support electronic screening and other roadside operations
- Perform electronic exchange using:
  - Electronic Data Interchange (EDI) standards
  - Non-EDI standards, the selection of which is system-dependent
  - New open standard methods of information exchange (e.g., XML) as they become available and are requested by users
- Allow the general public to access data without the security risk of providing a direct connection to sensitive legacy systems

CVIEW has similar Data Mailbox facilities as SAFER to facilitate the exchange of information among state users within the state agencies.

Citation & Accident
Record citation and accident data. This product may exist in some form in some states. Generally, the product is envisioned to perform these functions:

- Enter citation data electronically
- Issue citations
- Enter accident data electronically
- Generate accident reports
- Interface to CVIEW system (directly or through Roadside Ops) to report citations and accidents and access safety reports

Compliance Review (e.g. CAPRI)
Carrier Automated Performance Review Information. Compliance Reviews are on-site reviews of carriers and hazardous material shippers that cover compliance with critical parts of the Federal Motor Carrier Safety Regulations. The software that supports the electronic capture of compliance review data is called Carrier Automated Performance Review Information (CAPRI). CAPRI includes worksheets for collecting hours of service data, driver qualification data, and drug and alcohol compliance data. It creates preliminary carrier safety fitness rating and other reports for the motor carrier. Currently, CAPRI transmits completed compliance reviews to SAFETYNET via floppy disk transfer, or, if in a local area network environment, by storing a completed compliance review on a designated disk drive that SAFETYNET accesses directly. Future plans include being able to transfer compliance reviews from CAPRI to SAFETYNET via the SAFER Data Mailbox. This product was developed and is maintained by FMCSA. All Federal staff and most States use CAPRI software.

Description of State CV Credentials Administration System Components

Table 3-2 lists the CV Credentials Administration products in the generic CVISN state system design. The state should use this checklist to map the state's specific products to the generic components and to reflect the state's specific design.

Table 0-3 State CV Credentials Administration System Components

Commit Level (F/P/N)	System Name in Generic Design	System Name in Our State	Differences between Our State and the Generic Functions (+, -, none)	Comments
F	Web Site	OS/OW, COVERSNet	None	COVERSNet in Beta Test, Future Consolidation
F	Credentialing Interface	CI/MI	+	To Be Built
F	IFTA Registration	COVERSft	-	Need To Add Snapshots
F	IFTA Tax Filing	COVERSft	-	Need To Add Snapshots
F	IRP	COVERS	-	Need To Add Snapshots
F	Intrastate Vehicle Registration	ROS	None	Snapshot Update To Be Built
F	OS/OW	OS/OW	+	
F	Titling	ROS	None	Snapshot Update To Be Built
F	CDL/DL	CDL/DL	None	Snapshot Update To Be Built
P	Treasury System	DMV Revenue	-	Pilot In Progress. When Approved, Functionality Will Be Added. **Electronic Payment Not Part Of CVISN Level 1.** Even if EFT is involved, questionable whether DMV Revenue system would link in.
F	SSRS	SSRS	None	Snapshot Update To Be Built
N	HazMat			No System

The paragraphs in this section describe the functions of each CV Credentials Administration product in the generic CVISN state system design. The state should modify the paragraphs in this section to reflect its specific component names and functionality.

CRF 1048 authorized updating CVISN documents to reflect FMCSA's new policy on credentials administration. The policy change resulted from analyzing the results of a survey about electronic credentialing interactions between motor carriers and state information systems (see Reference 38). The new policy is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.
- FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.
- FMCSA encourages the exploration of XML as an alternative to EDI.

This is a policy regarding CVISN Level 1. If a state chooses to implement only a person-to-computer credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state chooses to implement only a computer-to-computer credentialing approach, then implementation of a person-to-computer interface is considered an Enhanced capability. The descriptions in this section have been updated accordingly.

Web Site

State Web site support for electronic credentialing. The carrier's credential applications will be submitted to the Web Site via an Internet browser. The Web Site would provide input screens and perform initial data checks. The Web Site would pass the application data to the Credentialing Interface, which would then route the application to the appropriate legacy system. The response from the legacy system would be returned to the carrier via the CI and Web Site.

- Provides on-line forms via a Web site
- Does initial error-checking on data entered onto forms
- Routes application data to the CI or directly to the appropriate state credentialing system
- Routes responses to the carrier
- May also archive transactions
- Provides temporary credentials, if feasible.
- May enable users to print credentials, for example, a mechanism to print once.

Credentialing Interface

The Credentialing Interface provides a convenient interface within the state to accept electronic credentialing application inputs from carriers, and to provide responses from state systems to carriers. As such, it is the focal point for credential and tax interaction with the carriers.

- Uses EDI ASC X12 standards or other format for interfaces with carriers
- Acknowledges receipt of valid EDI/non-EDI transactions
- Processes application data received from Web Site or CAT
- Archives transactions
- Does preliminary syntax checks on received transactions
- Allows for optional manual review of transactions
- Routes applications to the appropriate state credentialing system
- Routes responses to the carrier

A state may choose to extend the CI to perform some other function(s) normally allocated to another system, e.g., updating snapshot segments with credentials information.

IFTA

International Fuel Tax Agreement systems. See Reference 13. Usually split into two systems, one that handles ***registration*** and one that ***processes fuel tax returns***. The IFTA is a registration reciprocity agreement among states of the United States and provinces of Canada that provides for payment of fuel taxes on the basis of fuel used in various jurisdictions. Carriers pay fuel taxes to the various jurisdictions in which fleet vehicles are operated by registering and filing tax returns through a base state. Only one fuel use license is issued for each carrier when registered under the Agreement. In the generic CVISN state design, in addition to the normal IFTA functions, the IFTA Registration system also provides carrier snapshot updates.

IRP

International Registration Plan systems. See Reference 14. The International Registration Plan is a registration reciprocity agreement among states of the United States and provinces of Canada that provides for payment of interstate vehicle license fees on the basis of fleet miles operated in various jurisdictions. License fees are paid to the various jurisdictions in which fleet vehicles are operated through a base state. Only one license plate and one cab card is issued for each fleet vehicle when registered under the Plan. A fleet vehicle is known as an apportionable vehicle and such vehicle, so far as registration is concerned, may be operated both interjurisdictionally and intrajurisdictionally. In the generic CVISN state design, in addition to the normal IRP functions, the IRP system also provides carrier and vehicle snapshot updates.

Intrastate Vehicle Registration

These systems register commercial vehicles that normally operate within the state. In the generic CVISN state design, in addition to the normal intrastate vehicle registration functions, the system also provides vehicle snapshot updates.

OS/OW

Issue Oversize/Overweight permits. In the generic CVISN state design, in addition to the normal OS/OW functions, the OS/OW permitting system also provides carrier and vehicle snapshot updates.

Titling

Title new and used vehicles. In the generic CVISN state design, in addition to the normal titling functions, the Titling system will also provide vehicle snapshot updates.

CDL/DL

Issue Commercial Driver's License/ Driver's License. In the generic CVISN state design, in addition to the normal licensing functions, the system will also provide driver snapshot updates.

Treasury System

In this context, the State's Treasury system processes electronic payments. The Treasury system provides payment information to the credentialing system for which the fee/tax is paid. Various electronic payment methods are possible. States authorize electronic payment methods depending on regulations, capabilities, and experiences with individual payers.

SSRS
Single State Registration System. Carrier registration. The SSRS program was created to succeed the "bingo card" program administered by the Interstate Commerce Commission (ICC). The SSRS program is a base-State system whereby a motor carrier registers its interstate operating authority with, and provides proof of financial responsibility coverage to one State (a base-State) instead of multiple States. The base-State then distributes the collected fees to other participating States in which the motor carrier's vehicles operate. State participation in the System was limited to those States participating in the bingo card program prior to January 1991. Transportation agencies in 38 states register interstate authorities under the single state registration system (SSRS).

In the generic CVISN state design, in addition to the normal registration functions, the SSRS will also provide carrier snapshot updates.

HazMat
Hazardous Material registration and permitting. Provides for registration to carry HazMat and issues HazMat permits. In the generic CVISN state design, in addition to the normal HazMat functions, the HazMat system also provides carrier snapshot updates.

Description of State Electronic Screening System Components

Table 3-3 lists the Electronic Screening System products in the generic CVISN state system design. The state should use this checklist to map the state's specific products to the generic components and to reflect the state's specific design.

Table 0-4 State Electronic Screening System Components

Commit Level (F/P/N)	System Name in Generic Design	System Name in Our State	Differences between Our State and the Generic Functions (+, -, none)	Comments
F	Screening System	PrePass / IRD	None	Requires Coordination Of 3rd Party Data
F	Roadside Operations	PrePass / IRD / MCES	None	Pending PreVIEW Implementation
F	Sensor/Driver Communications	PrePass / IRD	-	No Height Detectors
F	E-Screening Enrollment	PrePass / WisDOT	None	Transponder ID An Issue

The paragraphs in this section describe the functions of each Electronic Screening System product in the generic CVISN state system design. The state should modify the paragraphs in this section to reflect its specific component names and functionality.

Each station's design is unique because of:

- State policy & practices
- Traffic flow, volume, & number of lanes
- Available site space
- Legacy system characteristics
- Existing proprietary solutions
- Vintage of roadside and communications equipment
- Resources available for making changes

Screening System
Make pass/pull-in decision.

- Interface to sensor/driver communications system
- Interface to Roadside Operations system (get snapshot summaries, send sensor data, send screening results)
- Sort vehicles on mainline or ramp, using: sensor data, snapshot data, availability of inspector, operator configuration selections
- Output screening results to tag via DSRC (includes driver notification)
- Control screening messages and signal lights
- Configure screening based on operator control (via Roadside Operations system) data
- Track vehicle through facility via tracking loops

Roadside Operations
Process snapshots and control site traffic.

- Interface to CVIEW – get snapshot data
- Support legacy operator interfaces (Static Scale, CDLIS, NLETS, Traffic Flow)
- Interface to electronic screening (send criteria, get screening results, get sensor data, send snapshot summaries)
- Interface to report activities from other roadside systems to infrastructure, and vice versa
- On request, retrieve report data and display
- Process snapshot data into local database
- Allow operators to set/view screening criteria
- Display sensor data to operator
- Display snapshot data to operator
- Display vehicle position data to operator (e.g. mainline, ramp, scale lane, inspection area)

Sensor/Driver Communications
Process vehicle measures and communicate via DSRC with driver.

- Weigh In Motion/Automatic Vehicle Classification
- Automatic Vehicle Identification (via DSRC)
- In-cab notification (via DSRC)
- Height detectors
- Static scales
- Variable message signs
- Signal lights

E-Screening Enrollment
This system is being prototyped in a few of the CVISN Model Deployment states. It will collect and evaluate requests from carriers to participate in electronic screening. It will provide the carrier with a mechanism to enroll in multiple electronic screening programs with a single application. (This section has been enhanced in accordance with CRF 1172.)

- Support the addition or removal of carriers and vehicles from e-screening programs
- Process carrier’s request for enrollment in one or more jurisdictions
- For own jurisdiction, evaluate carrier according to published criteria
- Process carrier’s request for participation of vehicles in one or more jurisdictions. Collect sufficient information to correlate carrier, vehicle, and transponder.
- Update carrier snapshot to show carrier’s request to participate in electronic screening in selected jurisdictions.
- Update carrier snapshot to show jurisdiction’s acceptance/rejection.
- Update vehicle snapshot to show carrier’s request to participate in electronic screening in selected jurisdictions.
- Update vehicle snapshot to show carrier, vehicle, and transponder IDs for jurisdictions as requested by the carrier.
- Update vehicle snapshots to show jurisdiction’s acceptance/rejection of carrier that is associated with vehicle.
- Share snapshots with other jurisdictions as carrier requests.

See the CVISN Guide to Electronic Screening [Reference 10] for further information.

references

1. JHU/APL, *ITS/CVO CVISN Glossary*, POR-96-6997 V1.0, dated December 1998.

2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists*, SSD/PL-99-0243, POR-97-7067 V 2.0, dated August 2000. The latest version will be available on the JHU/APL CVISN website http://www.jhuapl.edu/cvisn/.

3. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 - Project Management Checklists, POR-97-7067 P2.0, (Preliminary Version)*, September 1999. The latest version is available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

4. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists, POR-97-7067 D1.0, (Draft)*, April 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

5. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 - Interoperability Test Criteria, SSD/PL-99-0470, (Draft), dated July 1999*. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

6. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V1.0, (Baseline Version), March 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

7. JHU/APL, *Introductory Guide to CVISN, POR-99-7186 P.1 (Preliminary)*, May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

8. JHU/APL, *CVISN Guide to Safety Information Exchange, POR-99-7191, D.1*, March 2000. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

9. JHU/APL, *CVISN Guide to Credentials Administration, POR-99-7192, P.2*, August 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.

10. JHU/APL, *CVISN Guide to Electronic Screening, POR-99-7193, D.1*, October 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

11. JHU/APL, *CVISN Guide to Top-Level Design, POR-99-7187, P.1*, May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

12. Carol Gore, Federal Highway Administration Office of Motor Carriers - Field Systems Group (FSG) in Lakewood, CO, http://www.inspector.org/FMCSAfsg1.htm, a site maintained by the International Inspector’s Competition.

13. IFTA Articles of Agreement, last updated October 1998. Available from the IFTA Clearinghouse at their World Wide Web site http://www.iftach.org/Manual1.htm.

14. INTERNATIONAL REGISTRATION PLAN, INC. with official commentary, August 22, 1994. Available from IRP, Inc. at their World Wide Web site http://www.aamva.org/IRP/index.html.

15. JHU/APL, *SAFER User and System Requirements Document, draft Version 1.6,* SSD/PL-98-0503, September 1998. The latest version will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/.

16. The U. S. Department of Transportation, Federal Highway Administration, *Proposed Rule: Dedicated Short Range Communications In Intelligent Transportation Systems (ITS) Commercial Vehicle Operations*, 23 CFR Part 945, [FMCSA Docket No. FMCSA 99-5844] RIN 2125-AE63, published in Federal Register: December 30, 1999 (Volume 64, Number 250)], Page 73674-73742. Available from the Federal Register Online via GPO Access, http://www.access.gpo.gov/su_docs/aces/aces140.html [DOCID:fr30de99-43].

17. AASHTO (American Association of State Highway Transportation Officials), *Policy Resolution PR-14-97 Commercial Vehicle Electronic Screening Interoperability*, *AASHTO Transportation Policy Book*, January 1999. The document is available on the World Wide Web at http://www.aashto.org/.

18. The Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. II 1996) (amended 1997, 5 U.S.C.A. § 552a (West Supp. 1998)), which became effective on September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" which attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. An overview of the Privacy Act of 1974, prepared in September 1998 by the Office of Information and Privacy in coordination with the Office of Management and Budget is available on the Web at http://www.usdoj.gov/04foia/04_7_1.html.

19. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists, POR-97-7067 P1.0,* May 1999.

20. JHU/APL, Delivery of CVISN Electronic Credentialing Preference Survey Results, SSD-PL-00-0408, with enclosure Electronic Credentialing Preference Survey Results, June 2000, dated July 2000. This document is available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/.

21. FMCSA Field Systems Group, System Overview page of http://fmcsa-fsg.dot.gov/system_overview.htm.

A. Appendix A - Allocation of state systems design requirements

Tables in Chapter 4 of the COACH Part 1 listed the top-level requirements for the design of state systems in four categories:

- General
- Safety Information Exchange and Safety Assurance
- CV Credentials Administration
- Electronic Screening

In this chapter, the generic CVISN state design is summarized in a series of checklist tables, each of which corresponds to a table from COACH Part 1. In accordance with CRF 1204, this chapter has been updated to provide more guidance on how to use these tables. These tables were formerly included in Chapter 3.

The first and second columns ("Item #" and "Compatibility Criteria") in each table come from the COACH Part 1 Chapter 4 tables; these are the top-level requirements. The remaining columns correspond to components of the generic state design. The compatibility requirement level (L1, E, or C) in a cell indicates that the compatibility criterion is fulfilled in part or in whole by that component of the generic CVISN state design, and in what timeframe the criterion is expected to be implemented. If the item has been changed since the last revision, the next to last column indicates the Change Request Form (CRF) number for the CRF that triggered the document update. A list of all CRFs incorporated in this revision is included on the back of the title page. The last column provides a place for state-specific comments.

The columns of the checklist tables in this chapter must be modified by the state before they can be completed. In its own version of this document, each state should use the state-specific product names in the columns and/or add/delete design component columns. The completed checklists in Tables 3-1 through 3-3 of Chapter 3 contain the list of state-specific system components that should be used to modify the tables in this chapter.
Next, relabel the columns in the checklist tables (tables A.1-1 through A.4-1) and delete the columns the state is not using.

A.1 Allocation of General State Systems Design Requirements

The general state systems design requirements are allocated to all the systems that support the functions described by the compatibility criteria in Table A.1-1.

CRF 1048 authorized updating CVISN documents to reflect FMCSA's new policy on credentials administration. The policy change resulted from analyzing the results of a survey about electronic credentialing interactions between motor carriers and state information systems (see Reference 20). The new policy is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.
- FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.
- FMCSA encourages the exploration of XML as an alternative to EDI.

This is a policy regarding CVISN Level 1. If a state chooses to implement only a person-to-computer credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state chooses to implement only a computer-to-computer credentialing approach, then implementation of a person-to-computer interface is considered an Enhanced capability. The tables in this section have been updated accordingly.

The state should replace the component columns with the columns from its own layout, as described above, before completing the checklist.

Table A.1-1 Allocation of General State Systems Design Requirements Checklist

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.1.1	Adopt standard identifiers for carriers, vehicles, drivers, and transponders to support information exchange.	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X		
1	Adopt standard identifiers for interstate carrier, vehicle, driver, and transponder.	L1 F	L1 F	L1 F	E	L1 F	C	L1 F	L1 F	L1 F	L1 F		E	E	E		E	E	L1 F	L1 F	L1 F	E		
2	Adopt standard identifiers for intrastate carrier, vehicle, driver, and transponder.	C	C	C	C	C	C	C				C	C	C	C			C	C	C	C	C		
A.1.2	Use the World Wide Web for person-to-computer interactions between private citizens and state information systems.			L1 P	C		C	L1 F	L1 F	L1 F	*L1* *F*			E	*L1* *P*		E						1048 1164	Privacy Issues
A.1.3	Use open standards for computer-to-computer exchange of information with other jurisdictions and with the public.			L1; C	C		C	L1	L1	L1	*L1*			E	*L1*		E						1048 1164	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	Use ANSI X12 EDI standards for transactions between state information systems and private systems (CV operators, insurance companies, etc.).							L1 P																Pending Viable Alternative
2	Use ANSI X12 EDI standards for transactions between state information systems and CVISN Core Infrastructure systems, where available.			L1 F	C				L1 F	L1 *F*	*L1* *N*			E	*L1* *N*		E							AFF
3	Use XML standards for transactions between state information systems and private systems (CV operators, insurance companies, etc.) (contingent on demonstration of feasibility).		C	C	C		C	C																
A.1.4	Ensure that all information transfers, fee payments, and money transfers are authorized and secure.	L1 F	L1 F	L1 F	C	L1 F	C	L1 F	L1 F	L1 F	L1 F	E	E	E	E	L1 F	E	E	L1 F	L1 F	L1 F	E		

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.1.5	Exchange safety and credentials data electronically within the state to support credentialing, safety, and other roadside functions. Where useful, exchange snapshots.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		
1	Data for interstate carriers	L1 F	L1 F	L1 F	C	L1 F	C	L1 F	L1 F	L1 F	L1 F					L1 F	E	E	L1 F	L1 F		E		
2	Data for interstate vehicles	L1 F	L1 F	L1 F	C	L1 F		L1 F			L1 F		E	E		L1 F			L1 F	L1 F		E		
3	Data for intrastate carriers	E	E	E	C	E		E								E			E	E		E		
4	Data for intrastate vehicles	E	E	E	C	E		E				E	E	E		E			E	E		E		
5	Data for drivers	C	C	C	C										C	E			C	C				
A.1.6	Demonstrate technical interoperability by performing Interoperability Tests.	L1 F	L1 F	L1 F	C		C	L1 F	L1 F	L1 F	L1 F	E	E	E	C		E	E	L1 F	L1 F	L1 F	E		
A.1.7	Support electronic payments.						C	E	E	E	E	E	E	E		E	E	E				E		
A.1.8	Receive, collect, and archive relevant CVO data for historical, secondary, and non-real-time uses.						C	E	E	E	E	E	E	E		E	E	E				E	1047	

A.2 Allocation of State Safety Information Exchange and Safety Assurance Systems Design Requirements

Requirements from the COACH Part 1 Table 4.2-1 are allocated to specific products in Table A.2-1 below. The state should replace the component columns with the columns from its own layout, as described above, before completing the checklist.

Table A.2-1 Allocation of State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Siite	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.2.1	Use ASPEN (or equivalent) at all major inspection sites.		L1 F																					MCES
1	Select vehicles and drivers for inspection based on availability of inspector, standard inspection selection system (ISS), vehicle measures, and random process, as statutes permit.		L1 F																L1 F	L1 F				
2	Report interstate inspections to MCMIS via SAFETYNET.	L1 F	L1 F	L1 F																				
3	Report intrastate inspections to SAFETYNET.	L1 F	L1 F	L1 F																				
4	Submit interstate and intrastate inspections for 45-day storage to SAFER.		L1 F	L1 F																				

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Siite	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
5	Periodically check OOS orders issued in the state to focus enforcement and safety assurance activities.	E																						
6	To assist in inspection, use DSRC to retrieve summary vehicle safety sensor data, if driver allows and vehicle is properly equipped.		C																		C			
7	To assist in inspection, use DSRC to retrieve driver's daily log, if driver allows and vehicle is properly equipped.		C																		C			
8	Use electronically-generated driver's daily log, if driver offers as an alternative to a manually-maintained log during an inspection.		C																		C			
A.2.2	SAFETYNET 2000 submits interstate and intrastate inspections reports to SAFER.	L1 F																						Conversion From SAFETYNET In Process
A.2.3	Maintain snapshots (or equivalent information) for operators based in the state and make available to within-state information systems and users.			E																			827	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Siite	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	For any given snapshot, there is only one authoritative source (or group of authoritative sources, such as ASPEN units) for each field in that snapshot.			E																			827	
2	Allow only the authoritative source to update a snapshot data field, with the following exception: • A "super user" can update any field. An audit trail should be maintained to record super user updates.			E																			827	
3	Validate the sender's identity through some industry-standard means (account ID, IP address, password, security keys, . . .).			E																			827	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Siite	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
4	Reject updates attempted by any system other than the authoritative source or a super user with a code explaining why. The rejection transaction should be returned to the sender in a timely fashion. The rejection should be logged for the snapshot system administrator to review.			E																			827	
A.2.4	Use CAPRI (or equivalent) for compliance reviews.					L1 F																		
1	Report interstate compliance reviews to MCMIS via SAFETYNET.	L1 F				L1 F																		
A.2.5	Collect, store, analyze, and distribute citation data electronically.	L1, C P		C	C																			C - Report to SAFETYNET 2000 via CVIEW and SAFER Data Mailbox
1	Report citations for interstate operators to MCMIS via SAFETYNET.	L1, C P		C	C																			C - Report to SAFETYNET 2000 via CVIEW and SAFER Data Mailbox
A.2.6	Collect, store, analyze, and distribute crash data electronically.	L1, C P		C	C																			C - Report to SAFETYNET 2000 via CVIEW and SAFER Data Mailbox

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Siite	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	Report interstate crashes as required to MCMIS via SAFETYNET.	L1, C P		C	C																			C - Report to SAFETYNET 2000 via CVIEW and SAFER Data Mailbox
A.2.7	Compute carrier safety risk rating for intrastate carriers based on safety data collected.	E																						
A.2.8	Identify high risk drivers based in the state through regular performance evaluation of various factors such as license status, points, and inspections.	C																						

General Comment For A.2.5 and A.2.6: Initially, communication with SAFER will be via a direct connection using an AAMVA frame relay connection. Future development is a question – a lot depends upon the evolution of SAFETYNET 2000 and CVIEW

A.3 Allocation of State CV Credentials Administration Systems Design Requirements

Requirements from the COACH Part 1 Table 4.3-2 are allocated to specific products in Table A.3-1 below. The state should replace the component columns with the columns from its own layout, as described above, before completing the checklist.

CRF 1048 authorized updating CVISN documents to reflect FMCSA's new policy on credentials administration. The policy change resulted from analyzing the results of a survey about electronic credentialing interactions between motor carriers and state information systems (see Reference 38). The new policy is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.
- FMCSA recommends that, in the near term (over the next ~2 years), carriers and states use X12 EDI for computer-to-computer interfaces unless the state has evidence that customers support another approach.
- FMCSA encourages the exploration of XML as an alternative to EDI.

This is a policy regarding CVISN Level 1. If a state chooses to implement only a person-to-computer credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state chooses to implement only a computer-to-computer credentialing approach, then implementation of a person-to-computer interface is considered an Enhanced capability. The tables in this section have been updated accordingly.

When building a credentialing system, it is useful to think about the process of electronic screening enrollment as part of the design criteria. The allocation of requirements for Electronic Screening Enrollment have been moved to the section on Electronic Screening, since the enrollment would not occur unless operators wanted to participate in electronic screening. CRF 1172 authorized this change.

Table A.3-1 Allocation of State CV Credentials Administration Systems Design Requirements Checklist

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.3.1	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IRP.			L1			L1	L1			L1					L1							1048	
	Provide a Web site for a person-to-computer process.			L1 P			L1 F	L1 F			L1 F					L1 P							1048	COVERSNet & Additional Development
2	Provide a computer-to-computer automated process.			L1 P				L1 P			L1 P					L1 P							1048	Pending A Viable Standard
2a	Use EDI standards to provide a computer-to-computer automated process.			L1 F				L1 P			L1 F					L1 P							1048	Pending A Viable Standard
2b	Use XML standards to provide a computer-to-computer automated process.			E				E			C					C							1048	
A.3.2	Proactively provide updates to vehicle snapshots as needed when IRP credentials actions are taken.			L1 F							L1 F												1048 1164	Need To Add Snapshots

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	Interface to SAFER for interstate vehicle snapshots, using available SAFER interface.			L1 F																			1048 1164	Need To Add Snapshots
A.3.3	Proactively provide updates to carrier snapshots as needed when IRP credentials actions are taken.			L1 F							L1 F												1048 1164	Need To Add Snapshots
1	Interface to SAFER for interstate carrier snapshots, using available standards.			L1 F																			1048 1164	Need To Add Snapshots
A.3.4	Provide IRP Clearinghouse with IRP credential application information (recaps).										L1 F												313	Pending Joining Clearinghouse
A.3.5	Review fees billed and/or collected by a jurisdiction and the portion due other jurisdictions (remittance netting) as provided by the IRP Clearinghouse.										L1 F												313	Pending Joining Clearinghouse
A.3.6	Support electronic state-to-state fee payments via IRP Clearinghouse.										L1 F					L1 P								Pending Joining Clearinghouse

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.3.7	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IFTA registration.			L1 F			L1 F	L1 F	L1 F							L1 P							1048	
1	Provide a Web site for a person-to-computer process.			L1 P			L1 F	L1 P	L1 F							L1 P							1048	
2	Provide a computer-to-computer automated process.			L1 P				L1 P	L1 P							L1 P							1048	
2a	Use EDI standards to provide a computer-to-computer automated process.			L1 F				L1 P	L1 F							L1 P							1048	
2b	Use XML standards to provide a computer-to-computer automated process.			E				E	C							C							1048	
A.3.8	Proactively provide updates to carrier snapshots as needed when IFTA credentials actions are taken or tax payments are made.			L1 F					L1 F	L1 F													1048 1164	Need To Add Snapshots
1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface.			L1 F																			1048 1164	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.3.9	Provide IFTA Clearinghouse with IFTA credential application information using EDI standards.								L1 F															
A.3.10	Support electronic tax filing for IFTA quarterly fuel tax returns.			L1 F			L1 F	L1 P		L1 F						L1 P							1048	COVERSNet & Additional Development
1	Provide a Web site for a person-to-computer process.			L1 P			L1 F	L1 P		L1 F						L1 P							1048	COVERSNet & Additional Development
2	Provide a computer-to-computer automated process.			L1 P				L1 P		L1 P						L1 P							1048	
2a	Use EDI standards to provide a computer-to-computer automated process.			L1 F				L1 P		L1 F						L1 P							1048	
2b	Use XML standards to provide a computer-to-computer automated process.			E				E		C						C							1048	
A.3.11	Provide information on taxes collected by own jurisdiction and the portion due other jurisdictions (transmittals) to the IFTA Clearinghouse using EDI standards.									L1 F														
A.3.12	Download for automated review the demographic information from the IFTA Clearinghouse using EDI standards.									L1 F														

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.3.13	Download for automated review the transmittal information from the IFTA Clearinghouse using EDI standards.									L1 F														
A.3.14	Retrieve IFTA tax rate information electronically from IFTA, Inc.							L1 P		L1 F														Depends on IFTA, Inc. adding functionality.
A.3.15	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for other credentials.			E			C	E				E	E	E		E	E	E						
1	Interstate carrier registration			E			C	E								E	E							
2	Intrastate carrier registration			E			C	E								E								
3	Vehicle title			E			C	E						E		E								
4	Intrastate vehicle registration			E			C	E				E				E								
5	HazMat credentialing /permitting, if such credentials/permits are required by state law.			E			C	E								E		E						
6	Oversize/overweight permitting.			E			C F	E					E F			E P								
A.3.16	Proactively provide updates to vehicle snapshots as needed when credentials actions are taken.			E								E	E	E										

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	Vehicle title			E										E										
2	Intrastate vehicle registration			E								E												
3	Oversize/overweight permitting.			E									E											
A.3.17	Proactively provide updates to carrier snapshots as needed when credentials actions are taken.			E									E				E	E						
1	Interstate carrier registration			E													E							
2	Intrastate carrier registration			E																				
3	HazMat credentialing/permitting, if such credentials/permits are required by state law.			E														E						
4	Oversize/overweight permitting.			E									E											
A.3.18	Allow CV operators, government-operated, or third party systems to submit one or more applications in a single transaction.						C	E	E		E	E	E	E	E		E	E						Expect to handle multiple transactions for a single kind of credential (e.g. IRP).
A.3.19	Provide commercial driver information to other jurisdictions via CDLIS.														L1 F									
A.3.20	Evaluate safety performance prior to issuing credentials (i.e. support PRISM processes or equivalent).			E					E		E	E	E				E	E				E		

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.3.21	Allow carriers to provide information for audits electronically.									C	C	C												
A.3.22	Provide titling information to other jurisdictions via NMVTIS.													C										
A.3.23	Provide revoked IFTA motor carrier information to other jurisdictions via STOLEN.								C															
A.3.24	Accept electronic credential and supporting electronic documentation, in lieu of paper versions.		C	C	C				C		C	C	C	C	C		C	C		C		C		
A.3.25	Proactively provide updates to driver snapshots as needed when credentials actions are taken.			C											C									
1	Interface to SAFER for driver snapshots, using available SAFER interface.			C											C									

A.4 Allocation of State Electronic Screening Systems Design Requirements

Requirements from the COACH Part 1 Table 4.4-2 are allocated to specific products in Table A.4-1 below. The state should replace the component columns with the columns from its own layout, as described above, before completing the checklist.

The allocation of requirements for Electronic Screening Enrollment are included in this section.

Table A.4-1 Allocation of State Electronic Screening Systems Design Requirements Checklist

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.4.1	Follow FHWA guidelines for Dedicated Short Range Communications (DSRC) equipment.																		L1 F		L1 F		1159	PrePass
1	"For the immediate future, all CVO and Border crossing projects will continue to utilize the current DSRC configuration employed by the programs. This is the "ASTM version 6" active tag.																		L1 F		L1 F		115	PrePass
2	Beginning January 1, 2001, all CVO and Border Crossing projects will use a provisional standard as described below. In addition, this provisional standard will be designed to ensure interoperability with the existing legacy equipment used in CVO that conforms to ASTM Version 6.																		E		E		1159	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
2a	the new ASTM Physical Layer in the active mode;																		E		E		1159	
2b	the existing ASTM Version 6 Data Link layer in the synchronous mode.																		E		E		1159	
2c	and the IEEE 1455 Application Layer.																		E		E		1159	
A.4.2	Use snapshots updated by a SAFER/CVIEW subscription in an automated process to support screening decisions.			L1 F															L1 F	L1 F			1171	
1	Carrier snapshots.			L1 F															L1 F	L1 F				CVIEW / PreVIEW
2	Vehicle snapshots.			L1 F															L1 F	L1 F				CVIEW / PreVIEW
3	Driver snapshots.			C															C	C				
A.4.3	Implement interoperability policies as they are developed by ITS America, the American Association of State Highway Transportation Officials, HELP, Inc., MAPS, Advantage CVO, I-95 Corridor Coalition, and the Commercial Vehicle Safety Alliance.																		L1 F	L1 F				PrePass

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
1	See AASHTO's Commercial Vehicle Electronic Screening Interoperability Policy Resolution, PR-14-97, Reference 17.																		L1 F	L1 F				
A.4.4	Provide electronic mainline or ramp screening for transponder-equipped vehicles, and clear for bypass if carrier & vehicle were properly identified and screening criteria were passed.																		L1 F	L1 F	L1 F			PrePass
1	For transponder-equipped vehicles, identify carrier at mainline or ramp speeds.																		L1 F	L1 F	L1 F			Initially, only PrePass transponders
2	For transponder-equipped vehicles, identify vehicle at mainline or ramp speeds.																		L1 F	L1 F	L1 F			PrePass
3	Use WIM or weight history at mainline speed or on the ramp in making screening decisions.																		L1 F	L1 F	L1 F			PrePass / IRD
4	Record screening event data.																		E	E	E			
5	For transponder-equipped vehicles, identify driver at mainline or ramp speeds.																		C	C	C			
A.4.5	Collect from the carrier a list of jurisdictions and/or e-screening programs in which it wishes to participate in electronic screening and inform those jurisdictions and/or e-screening programs.																						1172	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.4.6	Collect from the carrier a list of jurisdictions and/or e-screening programs in which each of its vehicles chooses to participate in e-screening, and inform those jurisdictions and/or e-screening programs.																						1172	
A.4.7	Record transponder number and default carrier ID for each vehicle that intends to participate in e-screening.																						1172	
A.4.8	Share carrier ID for each carrier that intends to participate in e-screening with other jurisdictions and/or e-screening programs as requested by the carrier.																						1172	
1	Via SAFER snapshots																						1172	
A.4.9	Share transponder number and default carrier ID for each vehicle that intends to participate in e-screening with other jurisdictions, e-screening programs, or other agencies as requested by the carrier.																						1172	
1	Via SAFER snapshots																						1172	
A.4.10	Accept each qualified vehicle already equipped with a compatible transponder into your e-screening program without requiring an additional transponder.																						1172	
A.4.11	Enable the carrier to share information about the transponder that you issue with other jurisdictions, e-screening programs, or agencies.																						1172	

Item #	Compatibility Criteria	SAFETYNET	Inspections	CVIEW	Citation & Accident	Compliance Review	Web Site	Credentialing Interface	IFTA Registration	IFTA Tax Filing	IRP	Intrastate Veh Registr	OS/OW	Titling	CDL/DL	Treasury System	SSRS	HazMat	Screening System	Roadside Operations	Sensor/Driver Comm	E-Screening Enrollment	CRF #	Comments
A.4.12	Verify credentials/safety information with authoritative source prior to issuing citation.		L1, C F	C	C				L1, C F		L1, C F	L1, C F	L1, C F	L1, C F	L1, C F		L1, C F	L1, C		C F		L1, C F		L1 - via existing methods; C - via CVIEW Data Mailbox
A.4.13	If a vehicle illegally bypasses or leaves the CV check station, alert law enforcement for possible apprehension.																		C	C				
A.4.14	Report periodically to State safety information system on the activities conducted at each station (e.g. statistics).																		C	C				

NOTE to A.4.12: Wisconsin defines the authoritative source as a refreshed snapshot from SAFER.

Appendix D – COACH Part 4

Intelligent Transportation Systems (ITS)

Commercial Vehicle Operations (CVO)

CVISN Operational and Architectural Compatibility Handbook (COACH)

Part 4

Interface Specification Checklists

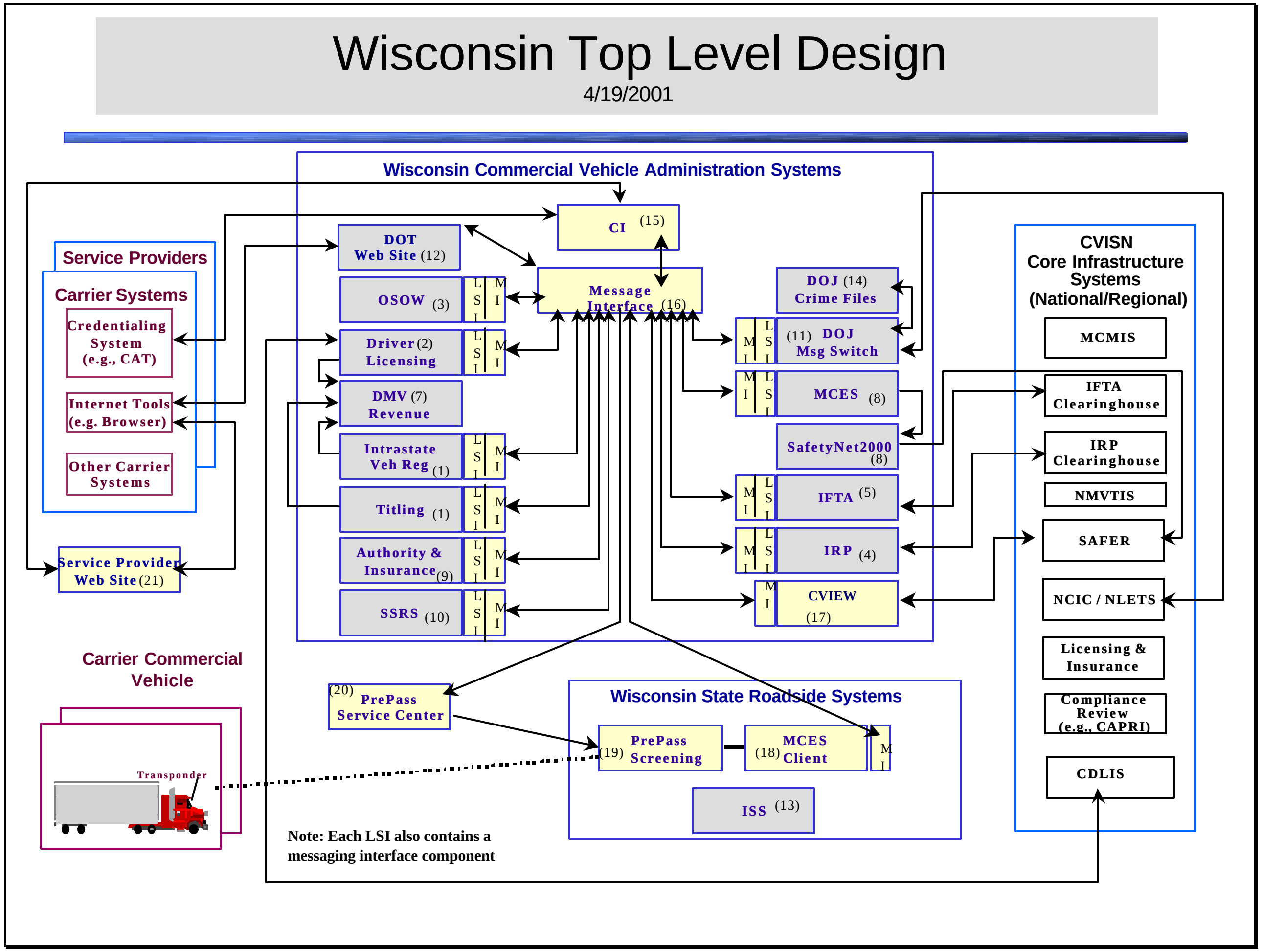
Preliminary Version

POR-97-7067 P2.0

October 2000

Wisconsin CVISN State System Design

Figure 0-1 Wisconsin State Design Template

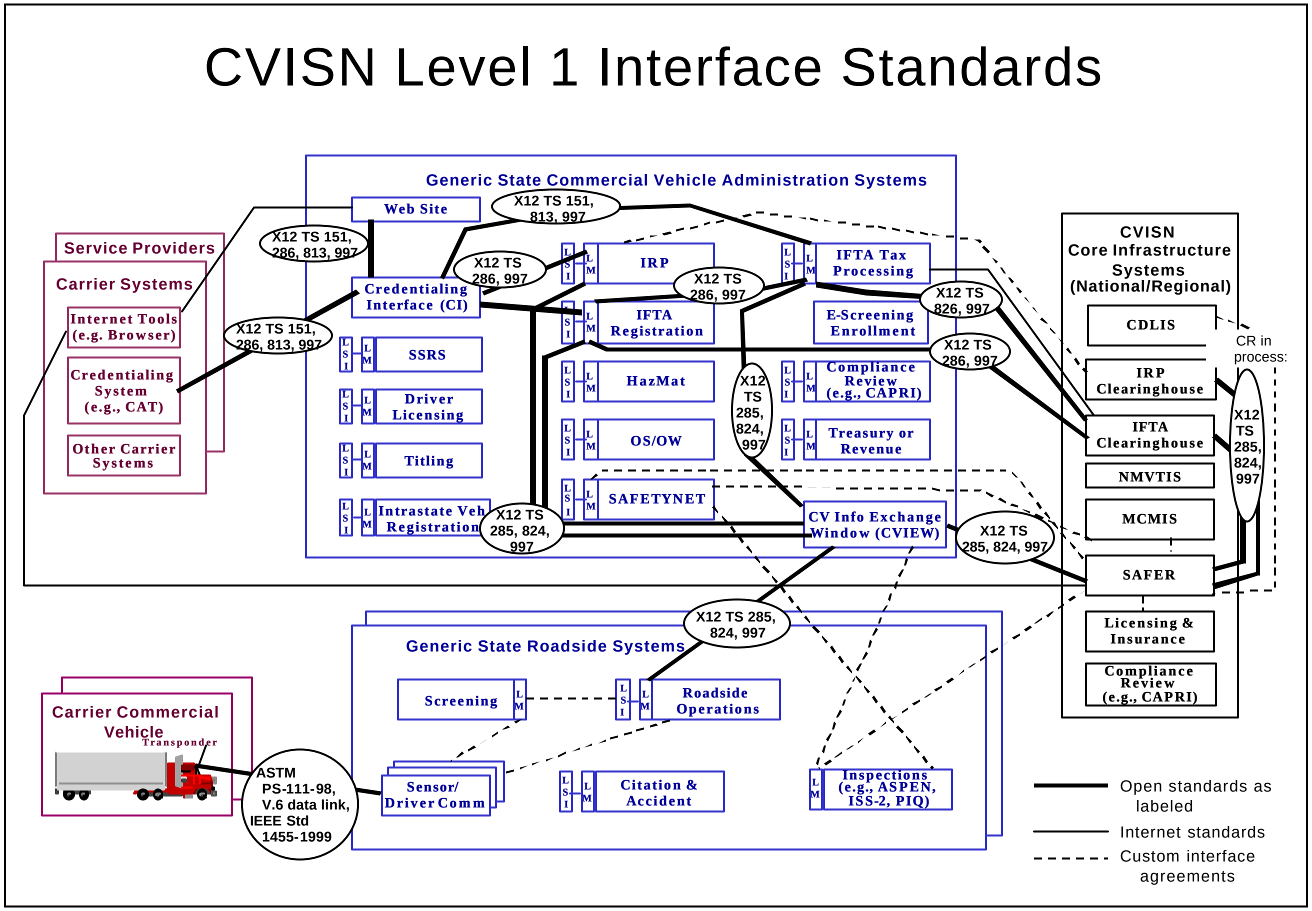


.

Standard interface identification

Figure 2-1 shows all the CVISN Level 1 interface standards overlaid onto the generic state design template. CRF 313, 1084, and 1159 have been applied. The **open standards shown in the ovals** are listed below:

Figure 0-2 CVISN Level 1 Interface Standards



CVISN Level 1 Interface Standards
Generic State Commercial Vehicle Administration Systems
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
CV Info Exchange Window (CVIEW)
LSI
LM
X12 TS 151, 813, 997
X12 TS 151, 286, 813, 997
X12 TS 286, 997
X12 TS 151, 286, 813, 997
X12 TS 286, 997
X12 TS 826, 997
X12 TS 286, 997
X12 TS 285, 824, 997
X12 TS 285, 824, 997
X12 TS 285, 824, 997
X12 TS 285, 824, 997
X12 TS 285, 824, 997
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
CR in process:
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
Carrier Commercial Vehicle
Transponder
ASTM PS-111-98, V.6 data link, IEEE Std 1455-1999
Open standards as labeled
Internet standards
Custom interface agreements

Figure 0-3 CVISN Level 1 Interface Functions

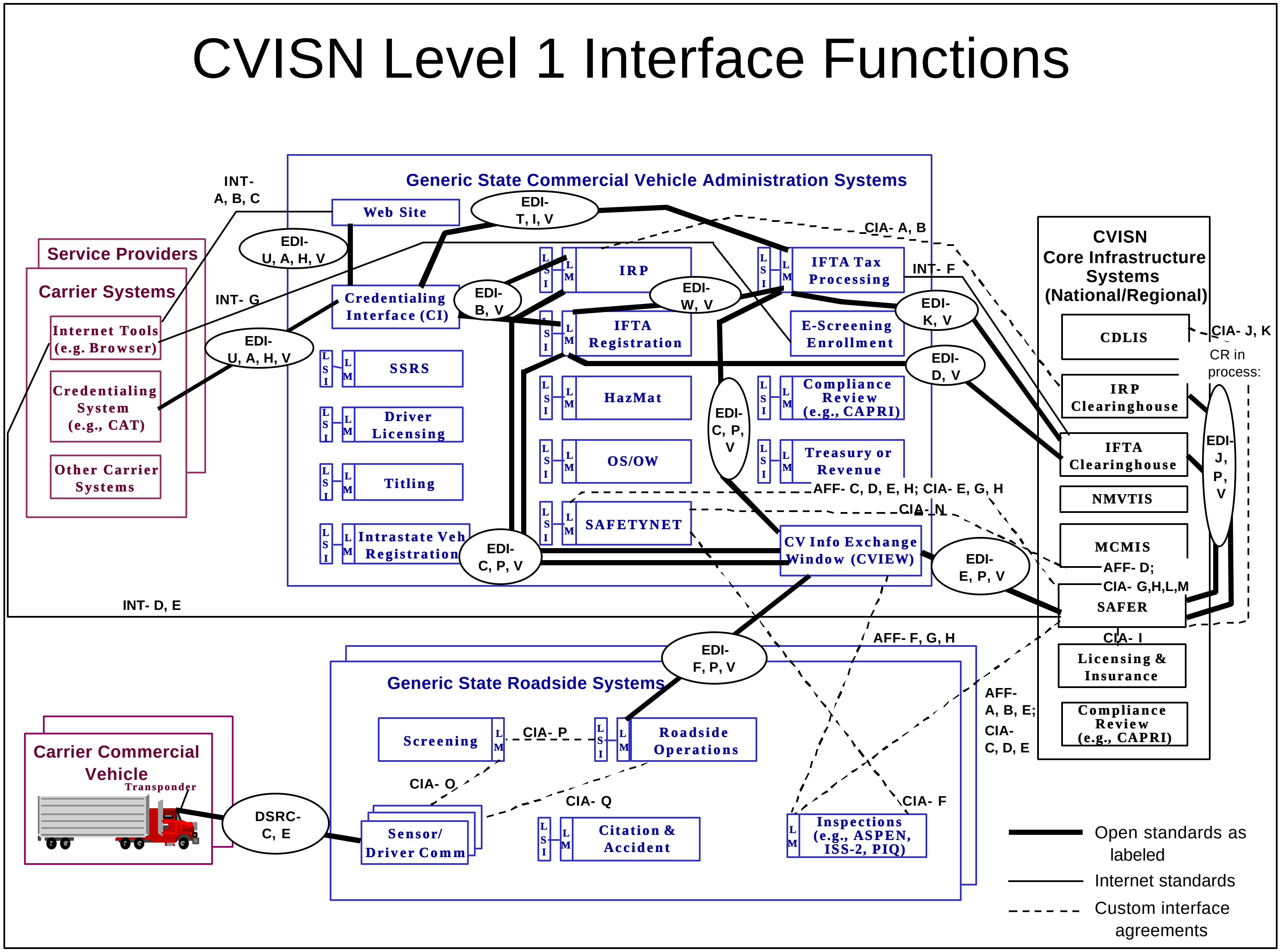


Table 0-1 Standard Interface Identification Table

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
F	EDI-A	TS 286 Ref 7, 9, 11, 12, 14	Commercial Vehicle (CV) Credentials: • Submit initial/renewal/supplemental electronic application for credentials • Submit trip permit application • Notify payee of payment method • Submit corrected application • Send renewal notice • Return credentials data to applicant • Return temporary credential • Return trip permit • Notify payer of fees due • Reject application	CAT (or Web Site) CAT (or Web Site) CAT (or Web Site) CAT (or Web Site) CI CI CI CI CI CI	CI CI CI CI CAT (or Web Site) CAT (or Web Site) CAT (or Web Site) CAT (or Web Site) CAT (or Web Site) CAT (or Web Site)	L1; E	L1 = IRP & IFTA E = other credentials Initial deployment will be via VPN directly to Polk systems. We want consistent data exchange between vendor systems and WisDOT. Currently, that is EDI. We would prefer XML.
F	EDI-B	TS 286 Ref 7, 9, 11, 12, 14	CV Credentials: • Pass application to legacy system • Return credentials data • Return temporary credential • Return trip permit • Report fees due • Reject application	CI Legacy admin system Legacy admin system Legacy admin system Legacy admin system Legacy admin system	Legacy admin system CI CI CI CI CI	L1; E	L1 = IRP & IFTA E = other credentials Legacy systems use AFF, Polk uses EDI.

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
N	EDI-C	TS 285 Ref 7, 13-14	CV Safety & Credentials Information Exchange: • Update snapshot segment • Request carrier, vehicle, or driver information (i.e. request a snapshot view) • Respond to carrier, vehicle, or driver information request or fulfill subscription (i.e. send one or more snapshots using a particular view)	Legacy admin system or E-screening Enrollment (or CI) Legacy admin system or E-screening Enrollment (or CI) CVIEW	CVIEW CVIEW Legacy admin system or E-screening Enrollment (or CI)	L1; C	L1 = carrier & vehicle C = driver CRF 1172 E=E-screening Enrollment AFF
F	EDI-D	TS 286 Ref 7, 11, 14	CV Credentials: • Submit application data • Retrieve demographic data from Clearinghouse for review	State IFTA Registration IFTA Clearinghouse	IFTA Clearinghouse State IFTA Registration	L1	COVERSft
F	EDI-E	TS 285 Ref 7, 13-14	CV Safety & Credentials Information Exchange: • Update snapshot segment • Request carrier, vehicle, or driver information (i.e. request a snapshot view) • Respond to carrier, vehicle, or driver information request or fulfill subscription (i.e. send one or more snapshots using a particular view) • Update snapshot segment	CVIEW CVIEW SAFER SAFER	SAFER SAFER CVIEW CVIEW	L1; C	L1 = carrier & vehicle C = driver

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
N	EDI-F	TS 285 Ref 7, 13-14	CV Safety & Credentials Information Exchange • Request carrier or vehicle information (i.e. request a snapshot view) • Respond to carrier or vehicle information request (i.e. send one or more snapshots using a particular view)	Roadside Operations CVIEW	CVIEW Roadside Operations	L1; C	L1 = carrier & vehicle C = driver AFF
	EDI-G		*deleted*				CRF 313
F	EDI-H	TS 813 Ref 7, 35	Tax Return: • File electronic IFTA tax return	CAT (or Web Site)	CI	L1	Initial deployment will be via VPN directly to Polk systems.
F	EDI-I	TS 813 Ref 7, 35	Tax Return: • Pass tax return to IFTA tax return processing system	CI	State IFTA Tax Processing System	L1	Initial deployment will be via VPN directly to Polk systems.
N/A	EDI-J	TS 285 Ref 7, 13-14	CV Safety & Credentials Information Exchange: • Update snapshot segment	IFTA or IRP Clearinghouse	SAFER	*L1*	NOTE: Change request in process for this to be implemented on behalf of states that belong to clearinghouse but are not yet CVISN states
F	EDI-K	TS 826 Ref 7, 36	Tax Information Exchange: • Send data on fuel tax filings among jurisdictions; summarize detailed tax information from individual returns and balance due/owed (netting and pre-netting summaries)	IFTA Clearinghouse	State IFTA Tax Processing System	L1	
	EDI-L	TS 150 Ref 7, 34	Tax Rate Notification • Send latest IFTA tax rates	CI	CAT or Web Site	E	
F	EDI-M	TS 284 Ref 7, 14, 31	CV Safety Reports (Inspection Report) • Submit safety report • Request safety report • Respond to safety report request	CVIEW CVIEW SAFER	SAFER SAFER CVIEW	*L1*	(not shown on figures; to support non-ASPEN Inspection systems)

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
N	EDI-N	TS 284 Ref 7, 14, 31	CV Safety Reports (Inspection Report) • Submit original safety report • Request safety report • Respond to safety report request	non-ASPEN Inspection system non-ASPEN Inspection system CVIEW	CVIEW CVIEW non-ASPEN Inspection system	*L1*	AFF
	EDI-O	TS 284 Ref 7, 14, 31	CV Safety Reports (Crash Data) • Submit original safety report	Citation & Accident	SAFETYNET 2000 via CVIEW & SDM	C	SDM = SAFER Data Mailbox
P	EDI-P	TS 824 Ref 7, 14, 40	Application Advice • Acknowledge successful processing of TS 285 update message data • Report errors in processing of TS 285 update message data	receiver of 285 receiver of 285	sender of 285 sender of 285	*L1*	When we accept a transaction, we'll respond. We would prefer XML.
	EDI-Q	TS 150 Ref 7, 34	Tax Rate Notification • Send latest IFTA tax rates	State IFTA Tax Processing System	CI	E	
	EDI-R	TS 286 Ref 41	Electronic Screening Enrollment • Submit e-screening enrollment data	CAT or other carrier system	E-Screening Enrollment	E	CRF 1172
	EDI-S	TS 820 Ref 7	Payment Order/Remittance Advice : • Initiate EFT payment • Report payment received	payer state's bank	payer's bank State Treasury or Revenue system	E	
P	EDI-T	TS 151 Ref 7, 32	Electronic Filing of Tax Return Data Acknowledgement • Report errors encountered when attempting to process IFTA tax return (813)	State IFTA Tax Processing System	CI	L1	

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
F	EDI-U	TS 151 Ref 7, 32	Electronic Filing of Tax Return Data Acknowledgement • Pass IFTA tax return error message • Pass IFTA tax return successfully processed message	CI CI	CAT (or Web Site) CAT (or Web Site)	L1	Initial deployment will be via VPN directly to Polk systems.
F	EDI-V	TS 997 Ref 7, 33	Acknowledge	all EDI-receiving systems	all EDI sending-systems	L1	Where applicable.
N/A	EDI-W	TS 286 Ref 7, 11, 14	CV Credentials: • Submit application data (complete or subset; (demographic information)	State IFTA Registration System	State IFTA Tax Processing System	L1	Same application.
N	EDI-X	TS 284 Ref 7, 14, 31	Inspection Report • Fulfill inspection report subscription • Query for inspection report • Respond to inspection query	SAFER Law Enforc User SAFER	Law Enforcement User SAFER Law Enforc User	*L1*	MCES via CVIEW.
	EDI-Y	TS 286 Ref 7, 11, 14	CV Credentials: • Query for latest credentials status • Respond to credentials query	Law Enforcement Credentialing System of record	Credentialing System of record Law Enforcement	E	

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
	DSRC	various	According to draft USDOT policy, • For the immediate future, all CVO and Border crossing projects will continue to utilize the current DSRC configuration employed by the programs. This is the "ASTM version 6" active tag. • Beginning January 1, 2001, all CVO and Border Crossing projects will use a provisional standard as described below. In addition, this provisional standard will be designed to ensure interoperability with the existing legacy equipment used in CVO that conforms to ASTM Version 6: a. the new ASTM Physical Layer in the active mode; b. the existing ASTM Version 6 Data Link layer in the synchronous mode; c. and the IEEE 1455 Application Layer.				CRF 1159
	DSRC-A	IEEE Std 1455-1999 Ref 24	CV Electronic Screening Message Set • CV Screening Identification	Transponder	Screening/Driver Comm	E	CRF 1159
	DSRC-B	IEEE Std 1455-1999 Ref 24	CV Screening Message Set All messages	Transponder or Screening/Driver Comm	Screening/Driver Comm or Transponder	C	CRF 1159
N/A	DSRC-C	IEEE Std 1455-1999 Ref 24	CV Border Clearance Message Set • Trip Identification Number message	Transponder	Screening/Driver Comm	L1	CRF 1159 No borders.
	DSRC-D	IEEE Std 1455-1999 Ref 24	CV Border Clearance Message Set All messages	Transponder or Screening/Driver Comm	Screening/Driver Comm or Transponder	C	CRF 1159

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
F	DSRC-E	ASTM 17.51 Ver 6 Ref 30	DSRC provisional standard	Transponder or Screening/Driver Comm	Screening/Driver Comm or Transponder	L1	CRF 1159 Depends upon PrePass.
	DSRC- F	ASTM 17.51 Ver 6 Ref 22	ASTM Physical Layer in the active mode	Transponder or Screening/Driver Comm	Screening/Driver Comm or Transponder	E	CRF 1159
	DSRC-G	ASTM 17.51 Ver 6 Ref 23	The existing ASTM version 6 Data Link Layer in the synchronous mode	Transponder or Screening/Driver Comm	Screening/Driver Comm or Transponder	E	CRF 1159
N	AFF-A	application file format Ref 25	Snapshot • Fulfill snapshot subscription • Query for snapshot(s) • Response to query	 SAFER ASPEN SAFER	 ASPEN SAFER ASPEN	*L1*	We will use CVIEW as the link to SAFER
N	AFF-B	application file format Ref 25	Inspection Report • Submit original inspection report • Query for inspection report • Respond to inspection query	 ASPEN ASPEN SAFER	 SAFER SAFER ASPEN	*L1*	MCES to SAFETYNET
N/A	AFF-C	application file format Ref 25	Snapshot • Fulfill snapshot subscription • Query for snapshot(s) • Response to query	 SAFER SAFETYNET 2000 SAFER	 SAFETYNET 2000 SAFER SAFETYNET 2000	*L1*	Federal systems capabilities
N/A	AFF-D	application file format Ref 25	Inspection Reports, Compliance Reviews, Crash Data, Enforcement Data • Update request (upload and store) • Update confirmation (confirm success)	 SAFETYNET 2000 MCMIS via SDM	 MCMIS via SDM SAFETYNET 2000	*L1*	SDM = Safer Data Mailbox Federal Systems

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
N	AFF-E	application file format Ref 25	Inspection Report • Submit original inspection report	ASPEN	SAFETYNET 2000 via SDM	*L1*	SDM = Safer Data Mailbox MCES to SAFETYNET 2000 – no SDM used.
F	AFF-F	application file format Ref 25	Snapshot • Fulfill snapshot subscription • Query for snapshot(s) • Response to query	CVIEW ASPEN CVIEW	ASPEN CVIEW ASPEN	*L1*	
F	AFF-G	application file format Ref 25, 26	Inspection Report • Submit original inspection report	ASPEN	SAFER via CVIEW	*L1*	Requires edit checks to be added to MCES client.
N	AFF-H	application file format Ref 25, 26	Inspection Report • Submit original inspection report	ASPEN	SAFETYNET 2000 via CVIEW & SDM	*L1*	SDM = Safer Data Mailbox MCES to SAFETYNET 2000 – no SDM or CVIEW used.

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
F	INT-A	Internet Standards	Equivalent of Commercial Vehicle (CV) Credentials: • Submit initial/renewal/supplemental electronic application for credentials • Submit trip permit application • Indicate payment method • Submit corrected application • Display vehicle inventory data (for renewal) • Display credentials data • Display temporary credential for printing • Display trip permit for printing • Display invoice • Display application rejection message	Internet Tools Internet Tools Internet Tools Internet Tools Web Site Web Site Web Site Web Site Web Site Web Site	Web Site Web Site Web Site Web Site Internet Tools Internet Tools Internet Tools Internet Tools Internet Tools Internet Tools	L1; E	L1 = IRP & IFTA E = other credentials CRF 1048
F	INT-B	Internet Standards	Tax Return: • File electronic IFTA tax return	Internet Tools	Web Site	*L1*	CRF 1048
F	INT-C	Internet Standards	Electronic Filing of Tax Return Data Acknowledgement • Display IFTA tax return error message • Display IFTA tax return successfully processed message	Web Site Web Site	Internet Tools Internet Tools	*L1*	CRF 1048
N/A	INT-D	Internet Standards	Snapshots • Query for snapshot(s) • Response to query	Internet Tools SAFER	SAFER Internet Tools	L1	Federal System
N/A	INT-E	Internet Standards	Inspection Reports • Query for inspection report • Respond to inspection query	Internet Tools SAFER	SAFER Internet Tools	*L1*	Federal System
F	INT-F	Internet Standards	Tax Rate Notification • Send latest IFTA tax rates	IFTA Clearinghouse	State IFTA Tax Processing System	L1	Download from Web site.
F	INT-G	Internet Standards	Electronic Screening Enrollment • Submit e-screening enrollment data	Internet Tools	E-Screening Enrollment	L1	CRF 1172

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
F	CIA-A	custom interface agreement	Recaps	State IRP	IRP Clearinghouse	L1	Need to join clearinghouse.
F	CIA-B	custom interface agreement	Netting/Transmittal data	IRP Clearinghouse	State IRP	L1	Need to join clearinghouse.
N	CIA-C	custom interface agreement Ref 25	Snapshots • Fulfill snapshot subscription • Query for snapshot(s) • Response to query	SAFER ASPEN SAFER	ASPEN SAFER ASPEN	L1	We will use CVIEW as the link to SAFER
N	CIA-D	custom interface agreement Ref 25	Inspection Reports • Submit original inspection report • Query for inspection report • Respond to inspection query	ASPEN ASPEN SAFER	SAFER SAFER ASPEN	L1	We will use CVIEW as the link to SAFER for submission of inspection reports.
N	CIA-E	custom interface agreement	Inspection Reports • Submit original inspection report	ASPEN	SAFETYNET via SDM	L1	SDM = Safer Data Mailbox Inspection reports will be submitted using MCES AFF routed to SAFETYNET.
N	CIA-F	custom interface agreement	Inspection Reports • Submit original inspection report	ASPEN	SAFETYNET via electronic bulletin board	L1	Inspection reports will be submitted using MCES AFF routed to SAFETYNET.
N/A	CIA-G	custom interface agreement Ref 25	Facsimile request Facsimile response	SAFETYNET MCMIS via SDM	MCMIS via SDM SAFETYNET	L1	SDM = Safer Data Mailbox Federal systems
N/A	CIA-H	custom interface agreement Ref 25	F-report request F-report response	SAFETYNET MCMIS via SDM	MCMIS via SDM SAFETYNET	L1	SDM = Safer Data Mailbox Federal systems
N/A	CIA-I	custom interface agreement Ref 25	Snapshot • Update carrier snapshot segment	Licensing & Insurance	SAFER	L1	Federal systems.

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
N/A	CIA-J	custom interface agreement Ref 25	Driver Status Report	CDLIS	SAFER	*L1*	Federal systems
N/A	CIA-K	custom interface agreement Ref 25	Driver History Report	CDLIS	SAFER	*L1*	Federal systems
N/A	CIA-L	custom interface agreement Ref 25	Snapshot • Update carrier snapshot segment	MCMIS	SAFER	L1	Federal systems
N/A	CIA-M	custom interface agreement Ref 25	Inspection Reports, Compliance Reviews, Crash Data, Enforcement Data • Provide past reports	MCMIS	SAFETYNET	L1	Federal systems
N/A	CIA-N	custom interface agreement Ref 25	Inspection Reports, Compliance Reviews, Crash Data, Enforcement Data • Provide reports	SAFETYNET	MCMIS	L1	Federal systems
F	CIA-O	custom interface agreement	Sensor data Control data	Sensor/Driver Comm Screening	Screening Sensor/Driver Comm	L1	PrePass
F	CIA-P	custom interface agreement	Screening criteria, snapshot data Screening results	Roadside Operations Screening	Screening Roadside Operations	L1	PrePass
F	CIA-Q	custom interface agreement	Sensor data Control data	Sensor/Driver Comm Roadside Operations	Roadside Operations Sensor/Driver Comm	L1	PrePass
	XML-tbd	W3C recommendation Ref 39	CV Safety & Credentials Information Exchange	tbd	tbd	E	CRF 1164 Specific information will be added at a later time.

Commit Level (F/P/N)	Label	Std	Interface Purpose	From System	To System	Reqts Level	Comments
	XML-tbd	W3C recommendation Ref 39	CV Credentials Information Exchange	tbd	tbd	E	CRF 1048 Specific information will be added at a later time.

NOTE: For CVISN Level 1,

- The credentials handled by TS 286 include IRP Registration and IFTA Registration; future credentials include Single State Registration/Unified Carrier Registration, Oversize/Overweight Permitting, HazMat Permitting, Vehicle Titling, Intrastate Vehicle Registration
- The snapshots handled by TS 285 include carrier (safety and credentials elements), vehicle (safety and credentials elements); future snapshots may include driver
- The safety reports handled by TS 284 include Inspection Results; future safety reports include HazMat Incident, Compliance Review, and Crash
- EDI interfaces are potential candidates for XML interfaces. This document will be updated to reflect XML interfaces after they have been prototyped by states.

Standard Data definitions

Ideally, there would be a common data dictionary for use throughout all systems associated with CVISN. That is not practical, since many legacy systems have different data definitions, and new systems are being developed by different organizations. Several documents define data elements that support CVO functions and standards [References 14, 21, 24, 27, 28, 29].

The data items listed in this chapter are common across more than one interface standard. They are used as "keys" to access information about the major entities: carrier, vehicle, driver, shipment, and trip. When systems use common keys, it is possible to match information sets such as safety and credentials data. The specifications in Table 3-1 define the key identifier characteristics to be adopted when exchanging information using the standards. It may be necessary to translate the identifier from a legacy system into this format when using a standard to exchange information. In addition to the standard column definitions explained in section 1.4, this table contains these columns:

- Entity – Any person, place, thing, concept, or event that has meaning to an enterprise, and about which data can be stored. (Example: vehicle)
- Identifier Name – the name of the data element that should be standard across systems for the entity
    - Identifier Segment – a list of components that make up the data name, including whether the segment should be alphabetic, numeric, or alphanumeric
- Number of Characters – the maximum length that should be supported for each segment

For further information about standard identifiers, see Reference 8.

Table 0-2 Standard Data Definitions

Commit Level (F/P/N)	Entity	Identifier Name	Identifier Segments	Number of Characters	Reqts Level	Comments
F	Motor Carrier	Primary Carrier ID e.g., For ***interstate*** carrier: MCI 12345 A001 (note that MCI is the code used for ID Type USDOT #) e.g., For ***intrastate*** carrier 0B US-CA 123A45689 1234 (note that 0B is the code used ID Type State-Specific)	ID Type (alphanumeric); if carrier is interstate, the type must be USDOT type code (MCI); for intrastate carrier without a USDOT number, the type code must be state-specific (0B) + Jurisdiction Code, if carrier is intrastate (alphanumeric); 2 character country code, hyphen, 2-character subdivision code; the allowable country and subdivision codes will be defined in the FMCSA Code Directory + Carrier-Specific Identifier corresponding to the ID type (alphanumeric); if carrier is interstate, must be USDOT number; if carrier is intrastate and has a USDOT number, must be USDOT number; for state-specific IDs, the Carrier-Specific Identifier may include a prefix to clarify the agency/source of the identifier) + Carrier Terminal ID designated by carrier (alphanumeric)	3 (max) 5 12 (max) 4 (max)	L1	USDOT number is required for entry into SAFER

Commit Level (F/P/N)	Entity	Identifier Name	Identifier Segments	Number of Characters	Reqts Level	Comments
F	Vehicle	Vehicle Identification Number e.g., 1FDKE30F8SHB33184 and Vehicle Plate ID e.g., US CA 12345664820M	VIN assigned by manufacturer (alphanumeric) Country code; the allowable country codes will be defined in the FMCSA Code Directory + Jurisdiction (state or province) code (alphanumeric); the allowable subdivision codes will be defined in the FMCSA Code Directory + License plate ID (alphanumeric)	30 (max) 2 2 12 (max)	L1	VIN may be too long. 17 characters is standard with an option for 2 additional for state use and/or 2 for a body not associated with a chassis. That would make a maximum of 21 characters.
F	Transponder	Transponder ID e.g., 0 123456789	Transponder ID Definition Flag (0=current; 1=IEEE P1455) + *If Transponder ID Definition Flag = current*, then the other segment is: Transponder Serial Number assigned by manufacturer *If Transponder ID Definition Flag = IEEE P1455*, then the other segments are: Manufacturer Identifier + Transponder Serial Number assigned by manufacturer	1 bit 32-bit hexadecimal value 16 bits; hexadecimal value 20 bits; hexadecimal value	L1 E	CRF 549 Via HELP, Inc.

Commit Level (F/P/N)	Entity	Identifier Name	Identifier Segments	Number of Characters	Reqts Level	Comments
P	Driver	Driver Unique ID e.g., US MD B99999999999A	Country code; the allowable country codes will be defined in the FMCSA Code Directory + Jurisdiction (state or province) code (alphanumeric); the allowable subdivision codes will be defined in the FMCSA Code Directory + Driver specific identifier (driver license number) assigned by jurisdiction (alphanumeric)	2 2 16 (max)	L1	The ID description is OK, but implementation may not be.
	Shipment	Shipment Unique ID e.g., 776655443322	Bill of Lading number assigned by the carrier (numeric)	12 (max)	C	
	Trip	Trip/Load Number e.g., 123456789761231	Carrier DUNS number as assigned by Dun and Bradstreet (numeric) + Trip unique number as assigned by carrier (numeric)	9 6	E	

Notes:

- In accordance with CRF 630, the Driver Unique ID has been updated to split country and subdivision.
- In accordance with CRF 631, the description of Trip/Load Number has been clarified to match IEEE Std 1455-99.
- In accordance with CRF 549, the Transponder ID is specified to be a two-part identifier, with the ID itself in hexadecimal representation.

references

1. JHU/APL, *ITS/CVO CVISN Glossary*, POR-96-6997 V1.0, dated December 1998.
2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists*, SSD/PL-99-0243, POR-97-7067 V 2.0, dated August 2000. The latest version will be available on the JHU/APL CVISN website http://www.jhuapl.edu/cvisn/.
3. *Reference Deleted*
4. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 - Project Management Checklists, POR-97-7067 P2.0, (Preliminary Version),* September 1999. The latest version is available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/.
5. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists, POR-97-7067 P2.0*, dated August 2000. The latest version will be available on the JHU/APL CVISN website http://www.jhuapl.edu/cvisn/.
6. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 - Interoperability Test Criteria, SSD/PL-99-0470, (Draft), dated July 1999*. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].
7. ANSI ASC X12, *Electronic Data Interchange X12 Standards*, Draft Version 4, Release 3, (a.k.a. Release 4030), December 1999.
8. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Recommendations for Common Carrier, Vehicle, Driver, and Cargo Identifiers*, SSD/PL-99-0388, June 1999. The latest version will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/.
9. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume I - IRP Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-96-6993 D.5, dated March 2000.
10. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume II – IRP Interstate Credential Transactions*, Draft Version, POR-96-6994 D.2, December 17, 1996.
11. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume III - International Fuel Tax Agreement (IFTA) Credential Transactions, ANSI ASC X12 Version 4 Release 3*, POR-97-6996 D.4, dated March 2000.
12. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume IV - Oversize / Overweight (OS/OW) Credential Transactions*, POR-97-7068 D.3, dated March 2000.
13. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Safety and Credentials Information Exchange (Transaction Set 285)*, POR-96-6995 D.5, dated March 2000.
14. JHU/APL, *Federal Highway Administration Code Directory*, POR-98-7127 D.5, dated March 2000.

15. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V2.0, (Baseline Version), August 2000. The latest version will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/

16. JHU/APL, *CVISN Guide to Top-Level Design*, POR-99-7187, to be published in 1999. The document will be available on the JHU/APL CVISN web site JHU/APL, *CVISN Guide to Top-Level Design*, *POR-99-7187, P.1*, May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

17. JHU/APL, *CVISN Guide to Safety Information Exchange, POR-99-7191, D.1*, March 2000. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

18. JHU/APL, *CVISN Guide to Credentials Administration, POR-99-7192, P.1*, July 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

19. JHU/APL, *CVISN Guide to Electronic Screening, POR-99-7193, D.1*, October 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/]

20. JHU/APL, *Introductory Guide to CVISN, POR-99-7186 P.1 (Preliminary)*, May 1999. [Note: This document is scheduled to be updated in 2000. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/].

21. American Association of Motor Vehicle Administrators (AAMVA), ANSI D20.1-1993, *States' Model Motorist Data Base, Data Element Dictionary, For Traffic Records Systems*, Second Edition, approved October 11, 1993

22. ASTM Preliminary Standard-111-98, Specification for Dedicated Short Range Communication (DSRC) Physical Layer using Microwave in the 920 to 928 MHz band, dated April 1999. For a summary of the standard, see http://www.its.dot.gov/standard/standard.htm.

23. ASTM Draft Standard for Dedicated, Short Range, Two-Way Vehicle to Roadside Communications Equipment, Draft 6, dated 23 February 1996.

24. IEEE Standard 1455-99, Standard for Message Sets for Vehicle/Roadside Communications, dated September 1999. For a summary of the standard, see http://www.its.dot.gov/standard/standard.htm.

25. JHU/APL, *SAFER System Interface Control Document*, version 2.0, POR-99-7129 D1.0, dated May 1999. The latest version will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/

26. JHU/APL, *CVIEW System Interface Control Document*, version 2.0, POR-99-7195 D1.0, dated May 1999. The latest version will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/

27. Data Interchange Standards Association (DISA), ANSI ASC X12.3, *Data Element Dictionary*, Draft Version 4, Release 2, document number ASC X12S/98-274, published December 1998.

28. National Safety Council, ANSI D16.1-1996, *Manual on Classification of Motor Vehicle Traffic Accidents*, Sixth Edition, approved October 28, 1996. (Provides "a common language" for users of traffic accident data and is "a standard for statistical classifications for motor vehicle traffic accidents.")

29. PB Farradyne, SAFETYNET 2000 Data Dictionary Version 0.0.5, published November 1998.

30. JHU/APL, *Delivery of Draft Specification for "Active Sandwich" Protocol for Dedicated Short Range Communications (DSRC) for Commercial Vehicles, SSD-PL-99-0784, with enclosure Draft Specification for DSRC for Commercial Vehicles, Version 0.0.1, November 1999*, dated December 1999.

31. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Safety Reports (Transaction Set 284)*, *Volume I – Inspection Reports Transactions, ANSI ASC X12, Version 4 Release 2*, POR-99-7202, D.2, dated March 2000. The document will be available on the JHU/APL CVISN web site http://www.jhuapl.edu/cvisn/.

32. Information about contacts regarding the use of TS 151, Electronic Filing of Tax Return Data Acknowledgment, is available at web site http://www.taxadmin.org/fta/edi/invedi.html.

33. Information about TS 997, Functional Acknowledgment, is available at web site http://snad.ncsl.nist.gov/dartg/edi/4010-ic.html.

34. Information about contacts regarding the use of TS 150, Tax Rate Notification, is available at web site http://www.taxadmin.org/fta/edi/invedi.html.

35. Information about TS 813, Electronic Filing of Tax Return Data, is available at web site http://www.taxadmin.org/fta/mf/.

36. Information about contacts regarding the use of TS 826, Tax Information Exchange, is available at web site http://www.taxadmin.org/fta/edi/invedi.html.

37. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists, POR-97-7067 D1.0, (Draft),* April 1999.

38. JHU/APL, *Delivery of CVISN Electronic Credentialing Preference Survey Results, SSD-PL-00-0408, with enclosure Electronic Credentialing Preference Survey Results*, June 2000, dated July 2000.

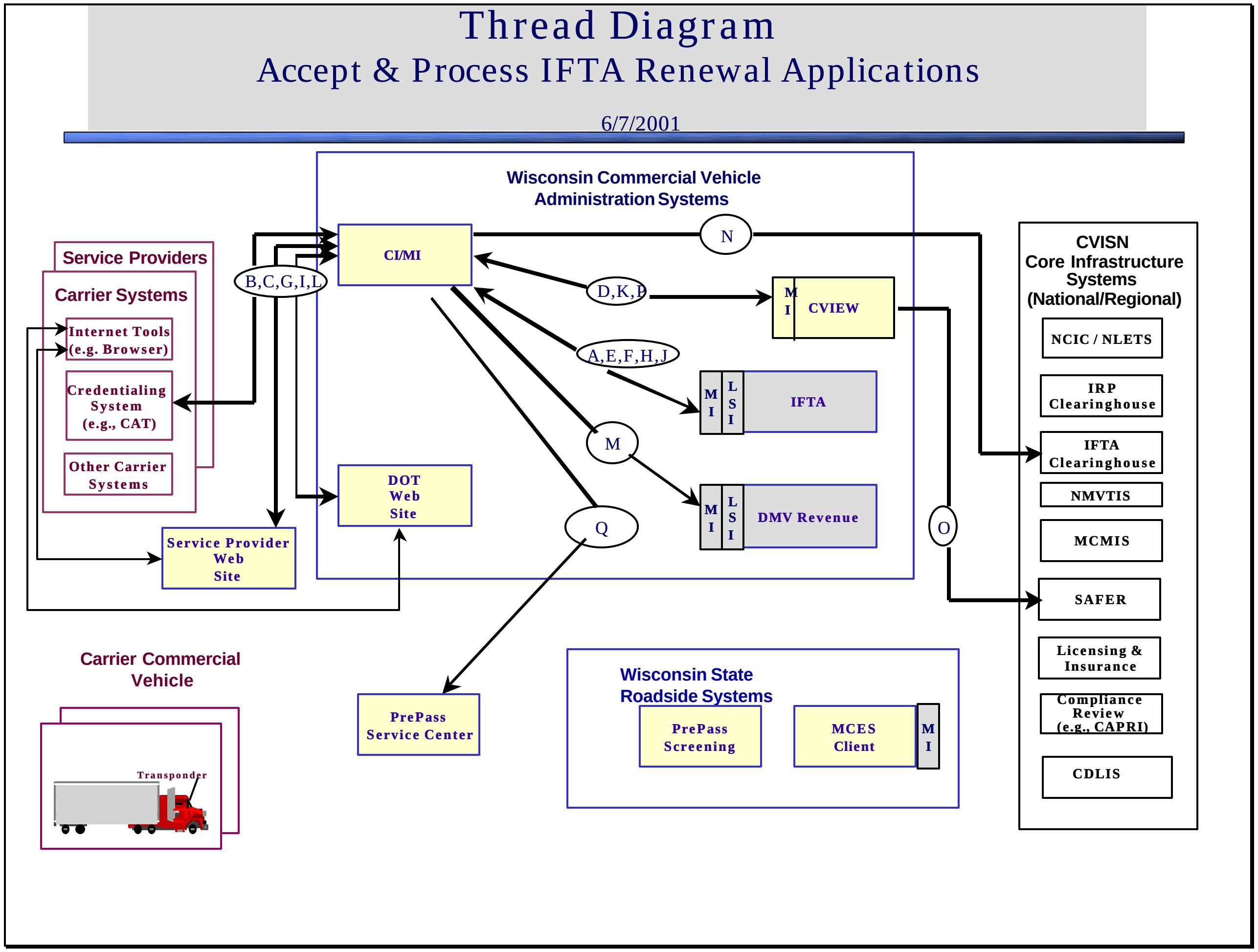
39. REC-xml-19980210, *Extensible Markup Language (XML) 1.0*, W3C Recommendation, dated February 10, 1998.

40. JHU/APL, *EDI Implementation Guide for Application Advice (Transaction Set 824), ANSI ASC X12 Version 4 Release 3*, POR-99-7203 D.2, dated March 2000.

41. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Credentials (Transaction Set 286), Volume VII - Electronic Screening Enrollment Transactions, ANSI ASC X12 Version 4 Release 3*, POR-99-7239 D.2, dated March 2000.

Appendix E – Operational Scenarios

Accept & Process IFTA Renewal Applications



Thread Diagram

Accept & Process IFTA Renewal Applications

6/7/2001

Wisconsin Commercial Vehicle Administration Systems

CI/MI

DOT Web Site

M I CVIEW

M I L S I IFTA

M I L S I DMV Revenue

Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

Service Provider Web Site

B,C,G,I,L

N

D,K,P

A,E,F,H,J

M

Q

O

CVISN Core Infrastructure Systems (National/Regional)

NCIC / NLETS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Carrier Commercial Vehicle

Transponder

PrePass Service Center

Wisconsin State Roadside Systems

PrePass Screening

MCES Client

M I

Scenario Description
Accept & Process IFTA Renewal Applications

A. Covers50 job (IFTA) generates the renewal form and puts on CI. (continue to mail to carriers not having electronic capability)

B. CI/MI ships package to carrier.

C. CI/MI receives renewal app from carrier. Depending on carrier preference, they may employ a CAT, the DOT Web Site or a service provider Web Site.

D. CI/MI uses application specific scripts to gather information from CVIEW needed by IFTA to process application.

E. CI/MI ships package to IFTA.

F. IFTA performs edits and status checks. If edits or status checks fail, IFTA rejects transaction, sending notification to CI/MI.

G. CI/MI forwards application rejection notification to carrier.

H. If IFTA finds application complete and status checks OK, IFTA processes application and shows amount due on system, and sends information to CI/MI.

I. CI/MI forwards billing information to carrier.

1. IFTA receives notification from state bank indicating deposit matches the amount due previously sent to carrier.

Scenario Description
Accept and Process IFTA Renewal Applications

J. IFTA assembles snapshot status summary for CVIEW, financial update for DMV Revenue, and application completed message for carrier and ships to CI/MI.

K. CI/MI sends snapshot status update to CVIEW.

L. CI/MI sends notification to carrier indicating IFTA renewal application has been successfully completed.

M. CI/MI sends financial update to DMV Revenue.

N. CI/MI sends snapshot status update to IFTA Clearinghouse for update.

O. CVIEW sends updated IFTA credential status to SAFER.

P. CVIEW sends updated IFTA credentials status to CI/MI for routing to Prepass PreView.

Q. CI/MI periodically routes updated IFTA credential status to PrePass PreView.

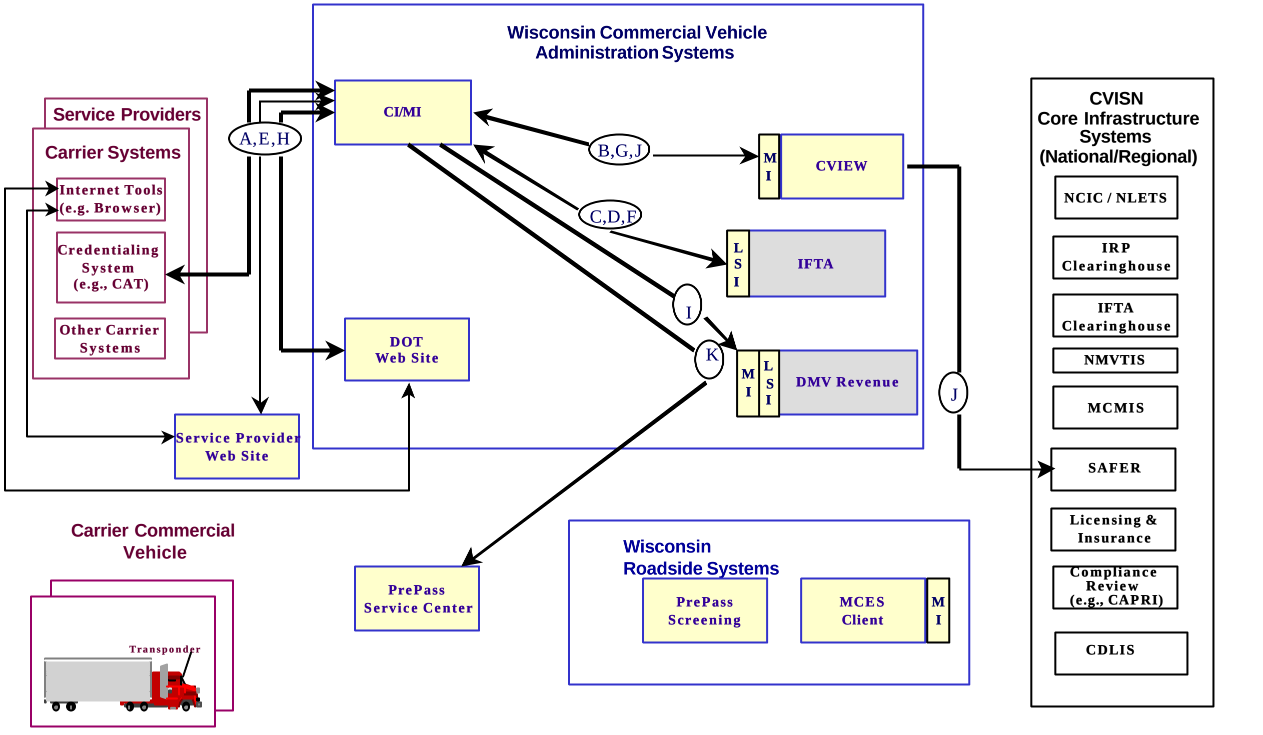
Note: Products and acknowledgements sent back to carrier browser are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Accept IFTA Application for Supplements

Thread Diagram

Accept IFTA Application for Supplements

6/14/2001



Scenario Descriptions
Accept IFTA Application for Supplements

A. Carrier electronically sends application for additional IFTA decal(s) to the CI/MI. Depending on carrier preference, they may employ a CAT, the DOT Web Site or a service provider Web Site.

B. CI/MI uses application specific scripts to gather information from CVIEW needed by IFTA to process application.

C. CI/MI routes carrier application & status information to IFTA.

D. IFTA performs edits and status checks. If edits or status checks fail, IFTA rejects transaction sending notification to CI/MI.

E. CI/MI forwards application rejection notification to carrier.

1. If IFTA finds application complete and status checks OK, IFTA processes application and calculates amount due.

2. IFTA receives notification from state bank indicating deposit matches the amount due for electronic transactions.

3. IFTA issues the decal(s). (Decal(s) mailed out manually).

F. IFTA assembles snapshot summary for CVIEW, financial update for DMV Revenue, & application complete message for carrier and ships package to CI/MI.

G. CI/MI sends update to CVIEW.

H. CI/MI sends application complete message to carrier.

Scenario Descriptions
Accept IFTA Application for Supplements

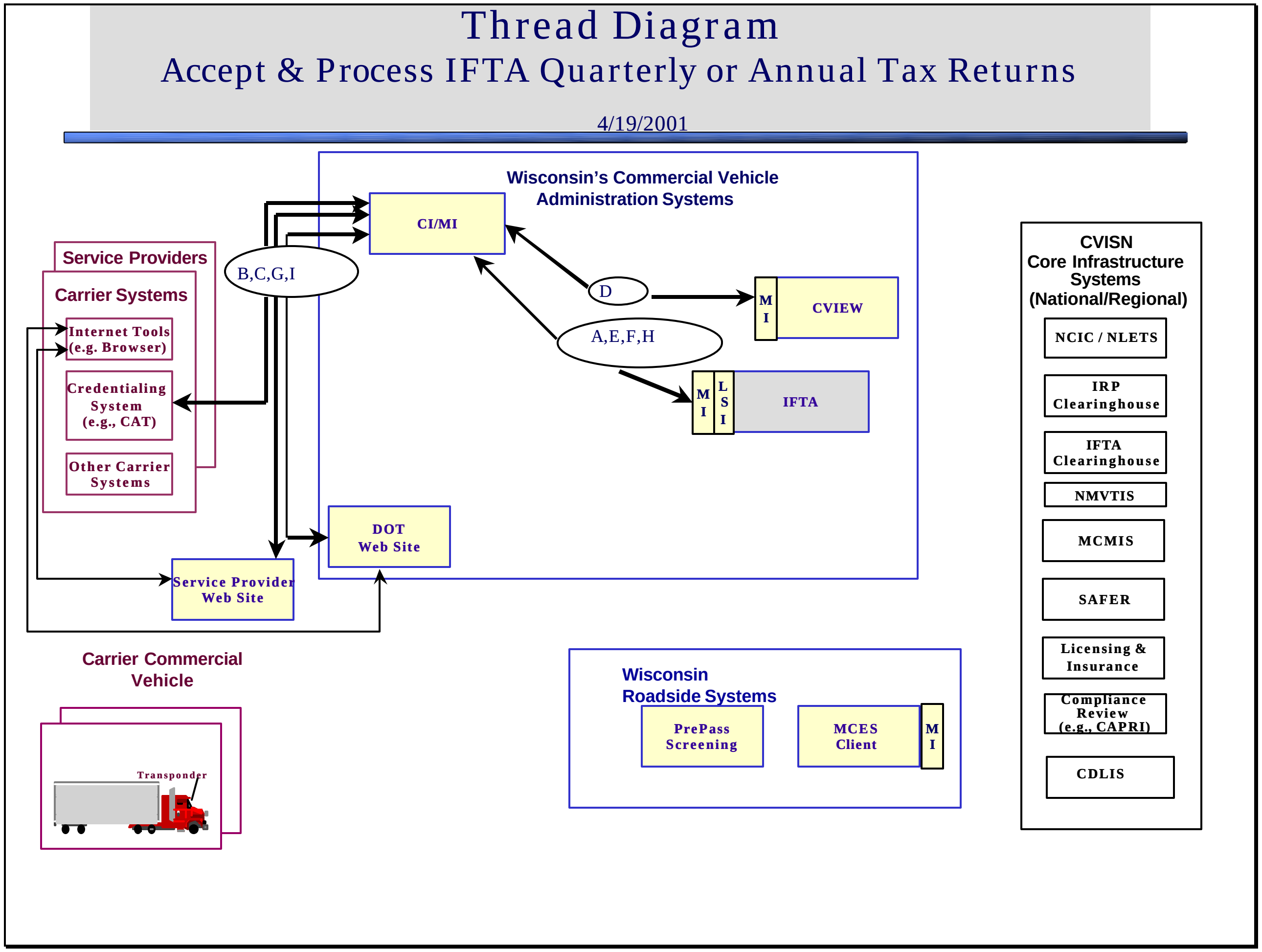
I. CI/MI sends financial update to DMV Revenue.

J. CVIEW sends update to SAFER.

K. CVIEW sends snapshot update to PrePass PreView via the CI/MI.

Note: Products and acknowledgements sent back to carrier browser are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Accept & Process IFTA Quarterly or Annual Tax Returns



Thread Diagram

Accept & Process IFTA Quarterly or Annual Tax Returns

4/19/2001

Wisconsin's Commercial Vehicle Administration Systems

CI/MI

CVIEW

IFTA

DOT Web Site

Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

Service Provider Web Site

Carrier Commercial Vehicle

Transponder

Wisconsin Roadside Systems

PrePass Screening

MCES Client

CVISN Core Infrastructure Systems (National/Regional)

NCIC / NLETS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Scenario Description
Accept & Process IFTA Quarterly or Annual Tax Returns

A. Batch job generates the tax return and sends to CI/MI. (continue to mail to carriers not having electronic capability)

B. CI/MI ships electronic return to carrier.

C. CI/MI receives electronic IFTA tax return from carrier. Depending on carrier preference, they may employ a CAT, the DOT Web Site, or a service provider Web Site.

D. CI/MI uses application specific scripts to gather status information from CVIEW needed by IFTA to process return (IFTA registration status, IRP registration status, valid account, return filing type).

E. CI/MI assembles the response from CVIEW & the carrier's electronic return and ships to IFTA.

F. IFTA performs edits and status checks. If edits or status checks fail, IFTA rejects transaction, sending notification to CI/MI.

G. Carrier receives electronic return rejection notice from CI/MI.
Note: Carrier will be required to resubmit the return again.

1. If IFTA finds return complete, IFTA processes the return & calculates the amount due or refund due.

H. IFTA sends carrier notification to CI/MI indicating amount due or amount to be refunded.

Scenario Description
Accept and Process IFTA Quarterly or Annual Tax Returns

I. Carrier receives amount due or to be refunded notification from CI/MI.

2. IFTA produces listing for MCSS staff detailing carrier amounts due or to be refunded.

3. MCSS processors notify IFTA when refund issued or payment is received. IFTA posts the refund or payment transaction on the IFTA system datab ase for the specific carrier.

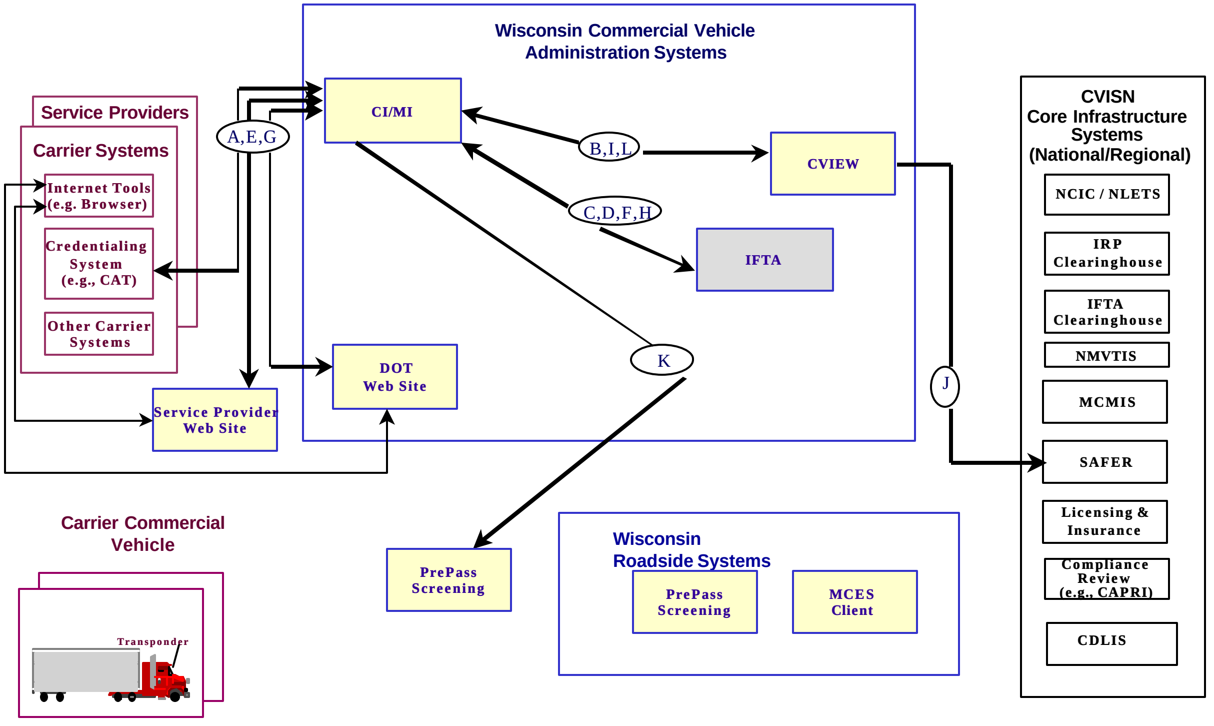
Note: Products and acknowledgements sent back to carrier browser are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Accept & Process IFTA Temporary Decal Request

Thread Diagram

Accept & Process IFTA Temporary Decal Request

4/23/2001


Wisconsin Commercial Vehicle Administration Systems
CI/MI
CVIEW
IFTA
DOT Web Site
B,I,L
C,D,F,H
A,E,G
K
J
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Service Provider Web Site
Carrier Commercial Vehicle
Transponder
PrePass Screening
Wisconsin Roadside Systems
PrePass Screening
MCES Client
CVISN Core Infrastructure Systems (National/Regional)
NCIC / NLETS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
CDLIS

Scenario Descriptions
Accept & Process IFTA Temporary Decal Request

A. Carrier electronically sends application for the temporary IFTA decal(s) to the CI/MI. Depending on carrier preference, they may employ a CAT, the DOT Web Site, or a service provider Web Site.

B. CI/MI uses application specific scripts to gather information from CVIEW needed by IFTA to process application. (IFTA registration, IRP registration, IRP VIN)

C. CI/MI assembles response from CVIEW and carrier's electronic application and routes information to IFTA.

D. IFTA performs edits and status checks. If edits or status checks fail, IFTA rejects transaction sending notification to CI/MI.

E. CI/MI forwards application rejection notification to carrier.

1. If IFTA finds application complete and status checks OK, IFTA processes application and shows zero dollars due on system. (temp IFTA decals are issued at no charge)

F. IFTA issues the temporary decal(s) and sends to CI/MI.

G. CI/MI forwards temporary IFTA decal(s) to carrier.

H. IFTA assembles snapshot summary update and ships package to CI/MI.

I. CI/MI sends snapshot summary update to CVIEW.

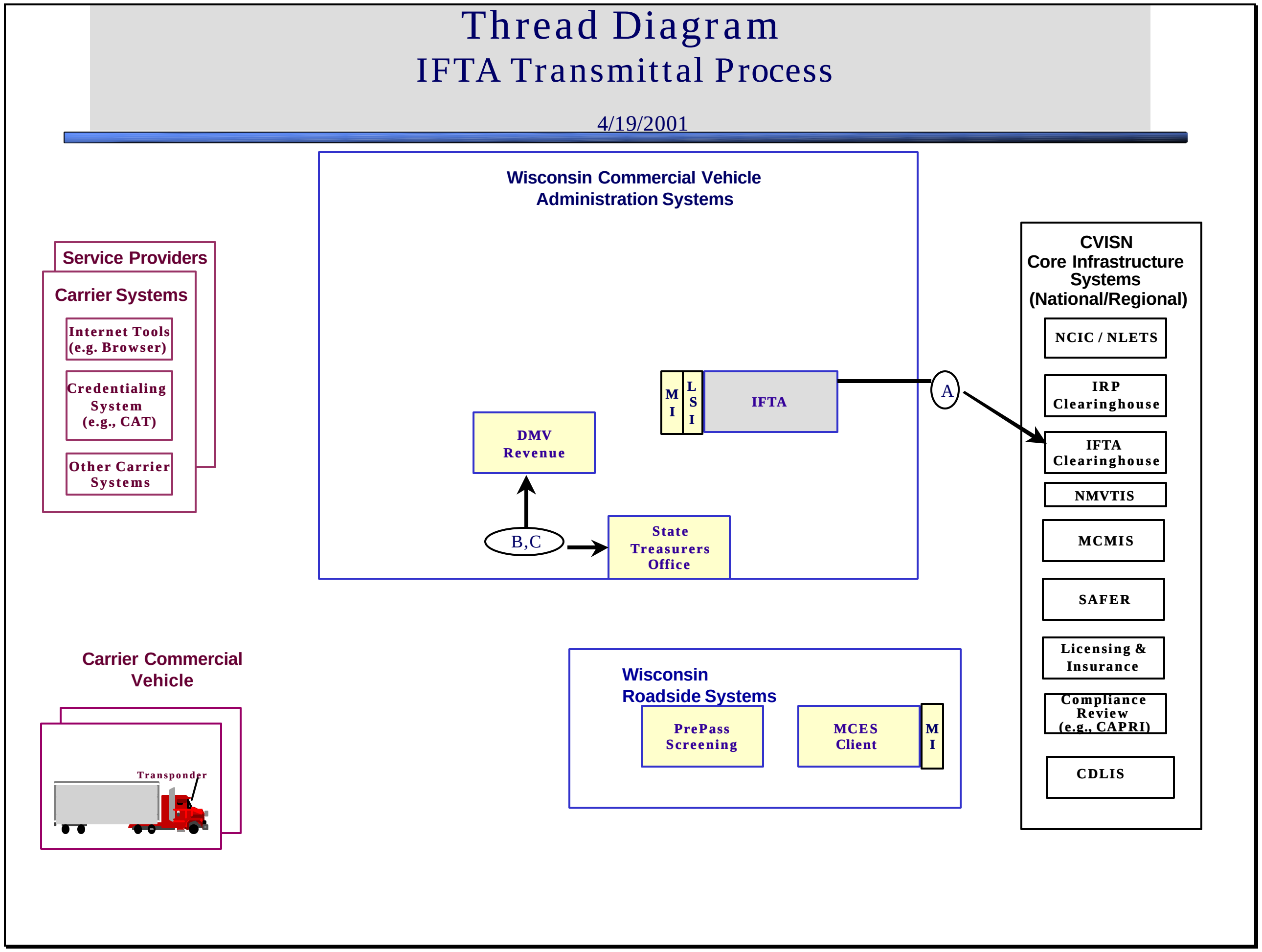
Scenario Descriptions
Accept & Process IFTA Temporary Decal Request

J. CVIEW sends update to SAFER.

K. CVIEW periodically sends snapshot updates to CI/MI for distribution to PrePass Preview.

Note: Products and acknowledgements sent back to carrier browser are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to C/MI connection.

IFTA Transmittal Process



Thread Diagram

IFTA Transmittal Process

4/19/2001

Wisconsin Commercial Vehicle Administration Systems
DMV Revenue
M I
L S I
IFTA
B,C
State Treasurers Office
A
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Carrier Commercial Vehicle
Transponder
Wisconsin Roadside Systems
PrePass Screening
MCES Client
M I
CVISN Core Infrastructure Systems (National/Regional)
NCIC / NLETS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
CDLIS

Scenario Descriptions
IFTA transmittal Process

1. **IFTA completed returns are available for selection for transmittals.**

2. **Upon request, IFTA batch job produces the transmittal.**

A. **IFTA transmittal data sent to IFTA Clearinghouse.**

3. **MCSS staff review clearinghouse totals and manually net the fees due between partner jurisdictions.**

4. **MCSS submits a manual request to the DMV Revenue system requesting the refund.**

B. **DMV Revenue system performs edit checks & triggers a refund request to State Treasurers office for issuance. State Treasurers office issues refund and sends acknowledgement to DMV Revenue system.**

5. **DMV Revenue system produces paper report for MCSS staff.**

C. **If refund request fails, State Treasurers Office sends failed status notification to DMV Revenue system.**

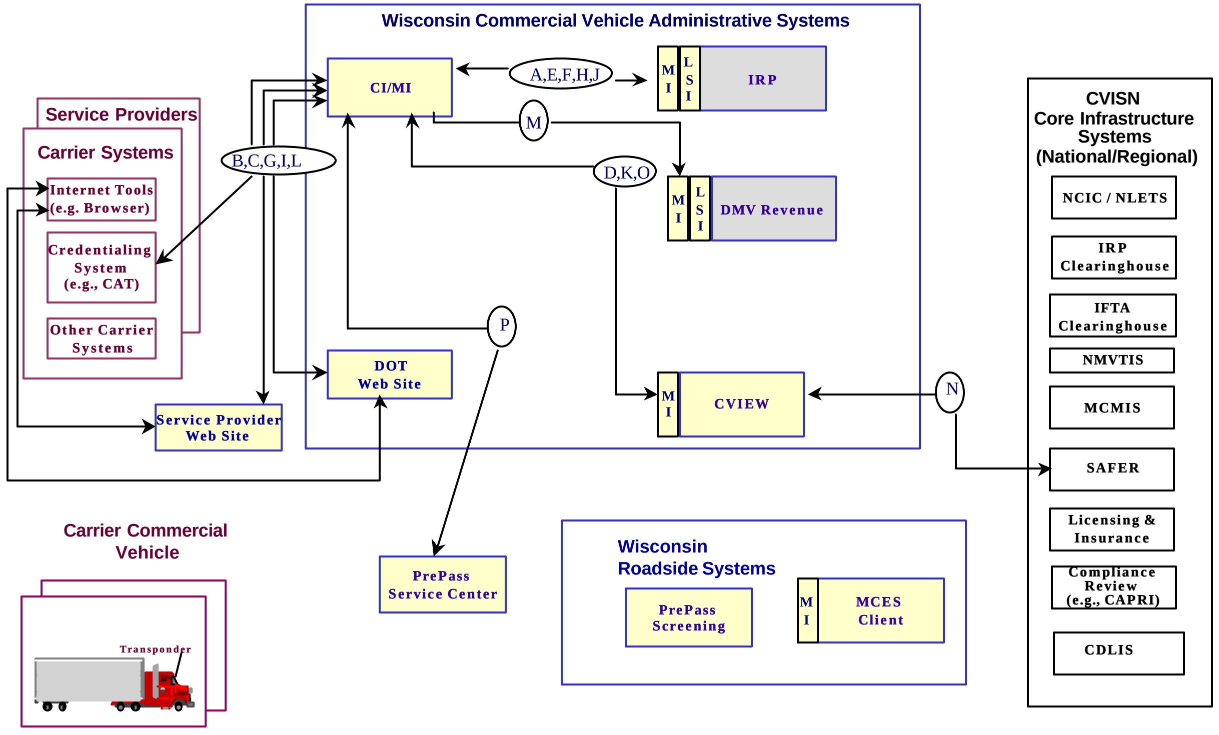
6. **DMV Revenue system produces paper report for MCSS staff indicating refund transaction failure.**

Accept & Process IRP Renewal Applications

Thread Diagram

Accept and Process IRP Renewal Applications

6/7/2001



Wisconsin Commercial Vehicle Administrative Systems

CI/MI

A,E,F,H,J

M I

L S I

IRP

M

D,K,O

DMV Revenue

B,C,G,I,L

Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

P

DOT Web Site

Service Provider Web Site

CVIEW

N

CVISN Core Infrastructure Systems (National/Regional)

NCIC / NLETS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Carrier Commercial Vehicle

Transponder

PrePass Service Center

Wisconsin Roadside Systems

PrePass Screening

MCES Client

Scenario Description
Accept & Process IRP Renewal Applications

A. Batch assembles renewal package and puts on CI/MI. (continue to mail to carriers not having electronic capability)

B. CI ships package to carrier.

1. Carrier submits paper copy (IRS form 2290) for proof of compliance for HVUT with a copy of both sides of their cancelled check.

2. Manual entry on IRP, Y/N field that HVUT proof provided and valid. This must be entered prior to a renewal being accepted. The processing system must indicate if fewer than 5,000 miles, number of vehicles and if less than 21 vehicles, list the VINS.

C. CI/MI receives application from carrier. Depending on carrier preference, they may employ a CAT, the DOT Web Site, or a service provider Web Site.

D. CI/MI uses application specific scripts to gather information from CVIEW needed by IRP to process application.

E. CI/MI forwards response from CVIEW and the carrier's application to IRP.

F. IRP performs edits and status checks. If edits or status checks fail, IRP rejects transaction, sending notification to carrier via CI/MI. If ok, sends receipt of transaction acknowledgement back to carrier via CI/MI.

G. CI forwards application rejection or acceptance notification to carrier.

H. If IRP finds application complete and status checks ok, IRP processes application and sends billing breakdown and / or TVR to CI/MI.

Scenario Description

Accept & Process IRP Renewal Applications

I. CI/MI forwards billing to carrier electronically.

3. IRP receives notification from state bank indicating deposit matches the billing breakdown previously sent to carrier.

4. IRP receives non-electronic payment of funds, processor indicating deposit matches billing previously sent to carrier.

J. IRP assembles snapshot status summary for CVIEW, financial update for DMV Revenue, and application completed message for carrier and ships package to CI/MI.

K. CI/MI sends snapshot status update to CVIEW.

L. CI/MI sends notification to carrier indicating IRP application has been successfully completed.

M. CI/MI sends financial update to DMV Revenue

N. CVIEW sends updated IRP credential status to SAFER.

O. CVIEW sends updated IRP credential status to CI/MI for routing to PrePass PreView.

P. CI/MI periodically routes updated IRP Credential status to PrePass PreView.

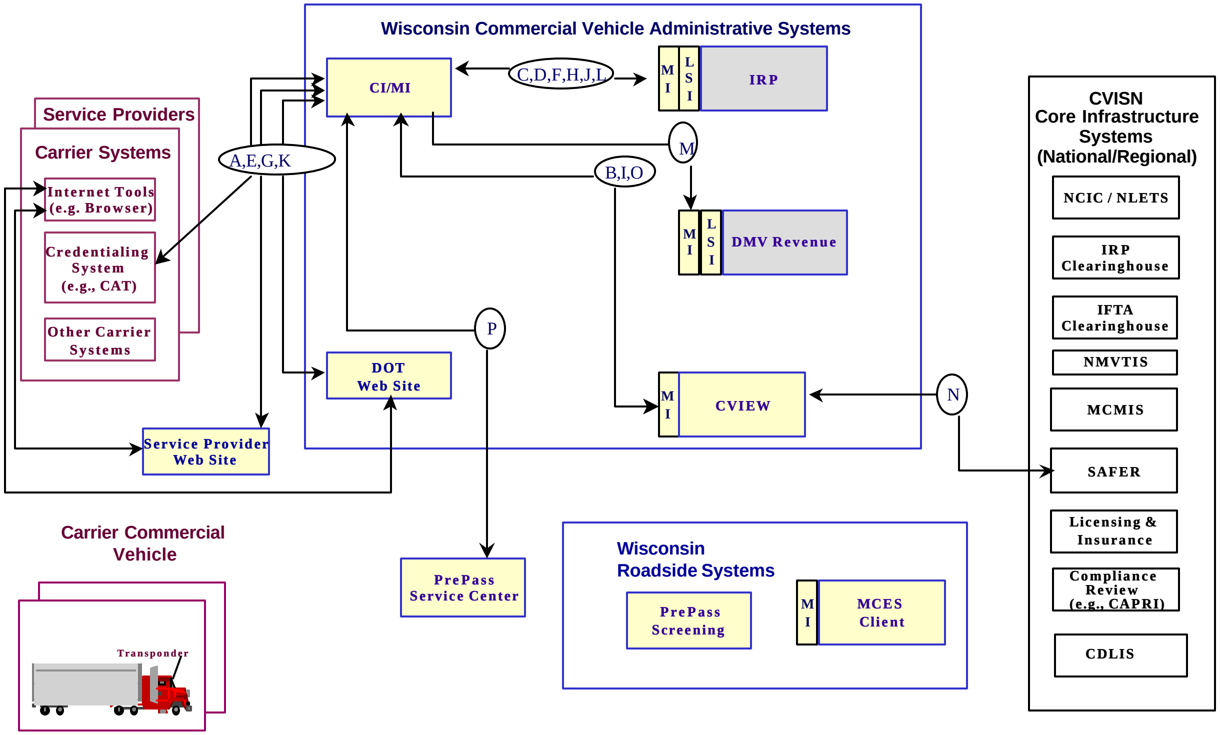
Note: Products and acknowledgements sent back to carrier browser are sent as mail attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Accept & Process IRP Supplement Applications

Thread Diagram

Accept and Process IRP Supplement Applications

6/6/2001



Scenario Description

Accept & Process IRP Supplement Applications

A. Carrier electronically sends application request to CI/MI. Depending on carrier preference they may employ a CAT, the DOT web Site or a service provider Web Site.

B. CI/MI uses application specific scripts to gather information (IRP account status) from CVIEW needed by IRP to process application.

C. CI assembles a package consisting of the response from CVIEW & the electronic application received from the carrier, and ships to IRP.

D. IRP performs edits and status checks. If edits or status checks fail, IRP rejects transaction, sending notification to CI/MI.

E Carrier receives supplement application rejection notification from the CI/MI.
Note: Rejected supplement application will not be posted to the IRP system.

F. If IRP finds supplemental application complete and status checks ok, IRP processes application and sends billing breakdown and / or TA to CI/MI.

G. Carrier receives billing information and / or TA from CI/MI.

1. IRP receives notification from state bank indicating deposit matches the billing.

H. IRP assembles snapshot status summary for CVIEW and ships to CI/ MI.

I. CI/MI sends IRP snapshot status update to CVIEW to update the CVIEW database.

Scenario Description

Accept & Process IRP Supplement Applications

J. IRP sends supplement application complete message to CI/MI for distribution to carrier.

K. Carrier receives supplement application successfully completed notification from CI/MI.

L. IRP sends financial update to CI/MI for routing to DMV Revenue.

M. DMV Revenue receives financial update from CI/MI.

N. CVIEW sends updated IRP credential snapshot status to SAFER.

O. CVIEW sends updated credential status to CI/MI for routing to PrePass PreView.

P. CI/MI periodically routes updated credential status to PrePass PreView.

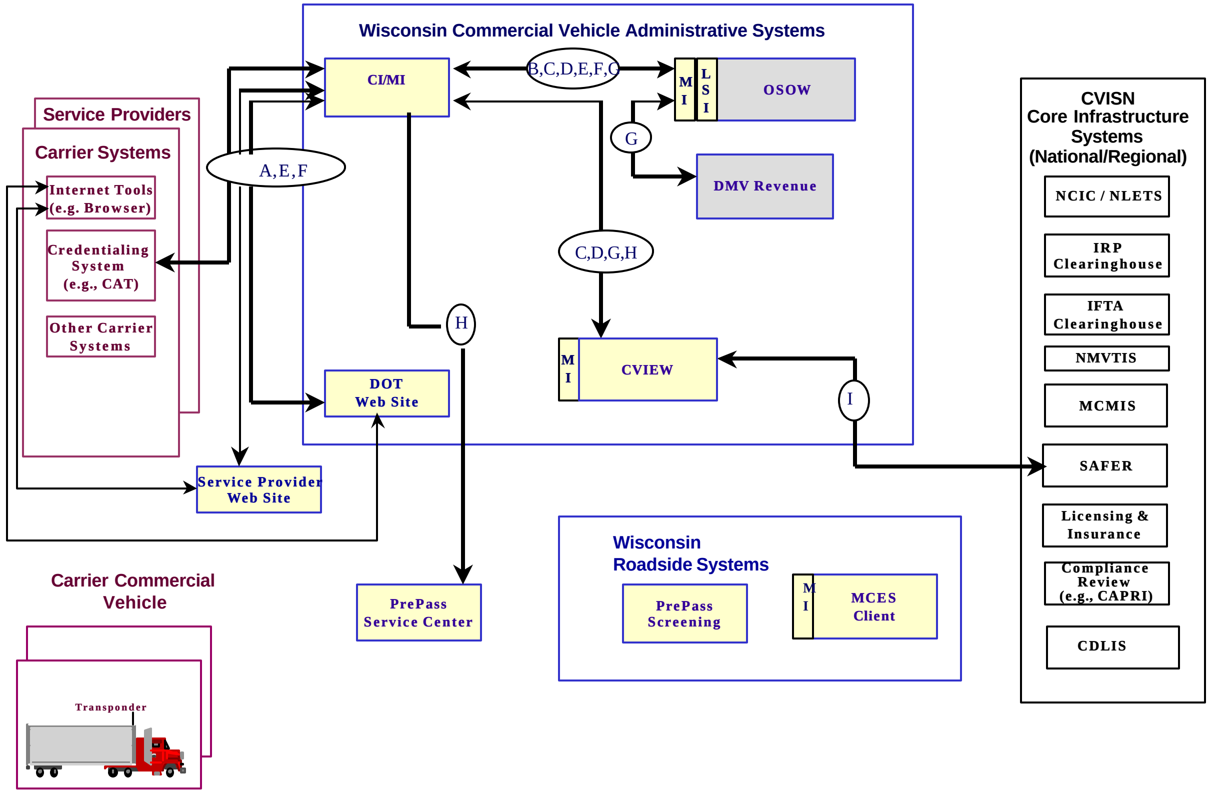
Note: Products and acknowledgements sent back to carrier browsers are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Issue New Oversize/Overweight Permit

Thread Diagram

Issue New Oversize/Overweight Permit

6/6/2001



Scenario Descriptions
(Issue New Oversize/Overweight Permit)

A. CI/MI receives application for oversize/overweight permit. Depending on carrier preference, they may employ a CAT, the DOT Web Site or a service provider Web Site.

B. CI/MI forwards application to Oversize/Overweight System (OSOW).

C. OSOW queries CVIEW via the CI/MI to verify credential information. If no information exists on CVIEW, CVIEW queries SAFER for credential snapshot.

D. OSOW receives query result back from CVIEW via the CI/MI.

E. If query results are OK, OSOW creates the permit, updates the DMV Revenue system, and transmits the permit image back to the CAT or Web site via the CI/MI.

F. If query results are not OK, OSOW sends a failure notification back to the CAT or Web site via the CI/MI.

G. OSOW updates CVIEW with permit information via the CI/MI.

H. CVIEW updates the PrePass Preview via the CI/MI at scheduled int ervals.

I. CVIEW updates SAFER at scheduled intervals.

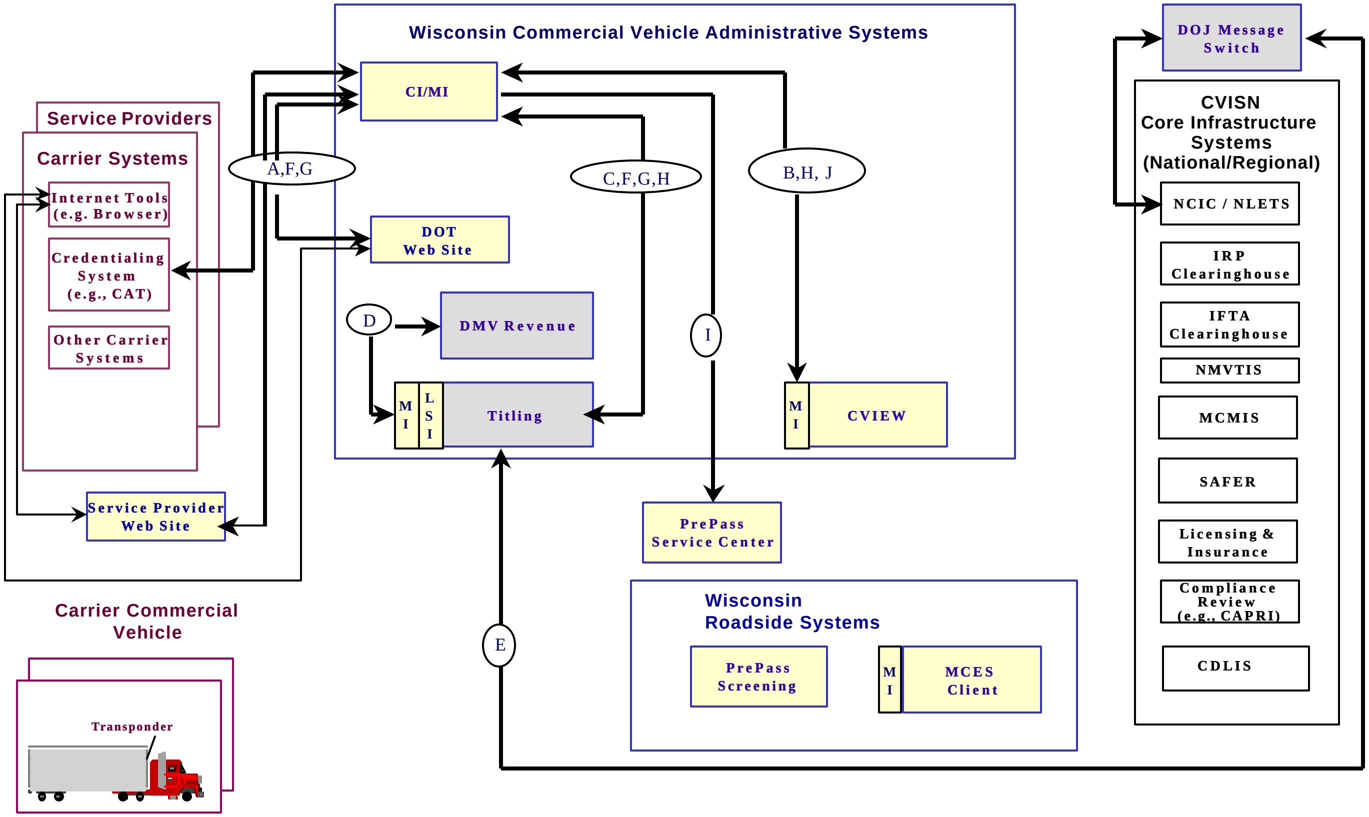
Note: Products and acknowledgements sent back to carrier browser are sent as email Attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Maintain Intrastate Carrier Snapshots

Thread Diagram

Maintain Intrastate Carrier Snapshots

4/19/2001



Scenario Description

Maintain Intrastate Carrier Snapshots

A. Carrier applies for title. Depending on carrier preference, they may employ a CAT, the DOT Web Site or a service provider Web Site.

B. CI/MI uses transaction specific script to send inquiry to CVIEW for authority and insurance status.

C. CI/MI uses transaction specific script to send ROS/ transaction to titling.

D. Titling system updates DMV Revenue System.

E. Titling System sends NCIC Query via DOJ Message Switch. Sometime up to a max of 72 hours later, NCIC responds to Titling system with stolen / not stolen status.

F. If not stolen, Titling System sends message to carrier via the CI/MI, notifying carrier we have application.

G. Titling system produces title and ships to carrier via the CI/MI.

H. Titling System updates the CVIEW via the CI/MI.

I. CVIEW periodically sends updates to PrePass PreView via the CI/MI.

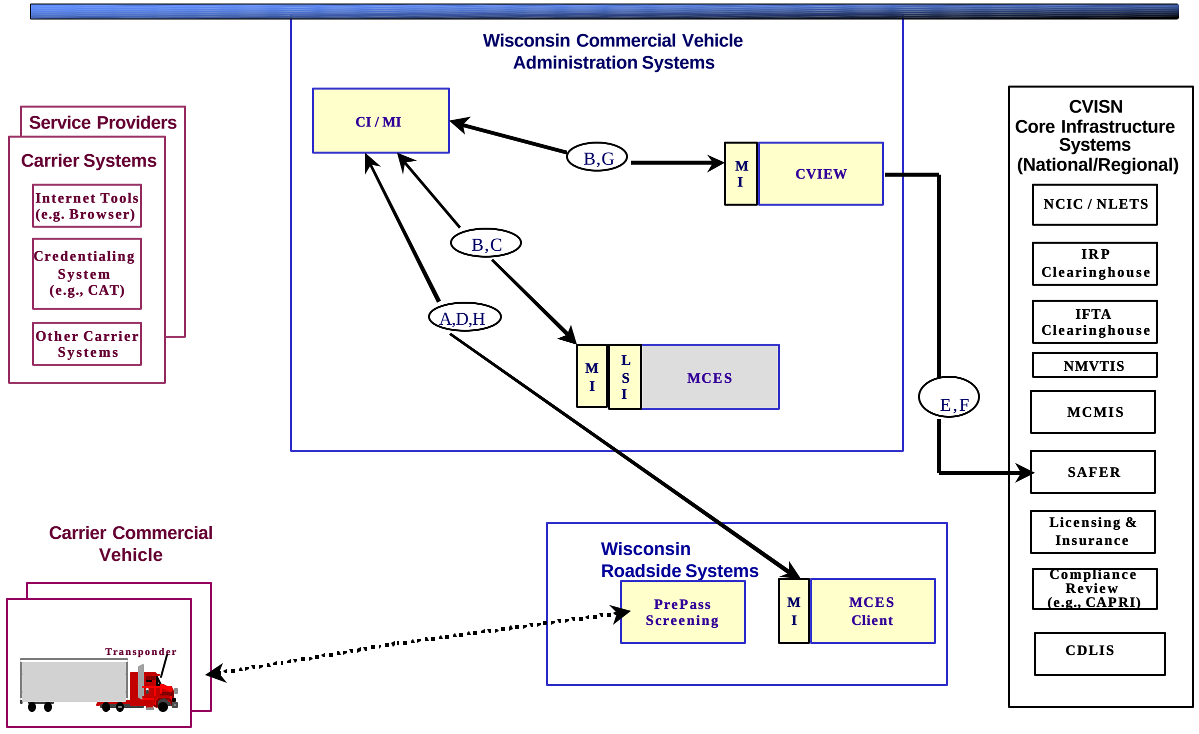
Note: Products and acknowledgements sent back to carrier browser are sent as email attachments. For CAT interface, CI/MI will queue responses until carrier re-establishes a CAT to CI/MI connection.

Query for Past Inspection Report - PIQ

Thread Diagram

Query for Past Inspection Report – PIQ

4/19/2001



Wisconsin Commercial Vehicle Administration Systems

CI / MI

B,G

M I

CVIEW

B,C

A,D,H

M I

L S I

MCES

E,F

Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

CVISN Core Infrastructure Systems (National/Regional)

NCIC / NLETS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Carrier Commercial Vehicle

Transponder

Wisconsin Roadside Systems

PrePass Screening

M I

MCES Client

Scenario Description
Query for Past Inspection Report - PIQ

A. MCES Client routes inspection query to CI/MI using plate # as key.

B. CI/MI uses transaction specific script to route query to MCES and CVIEW.

C. MCES responds with inspection report(s) or not found to CI/MI.

D. CI/MI routes response to MCES Client.

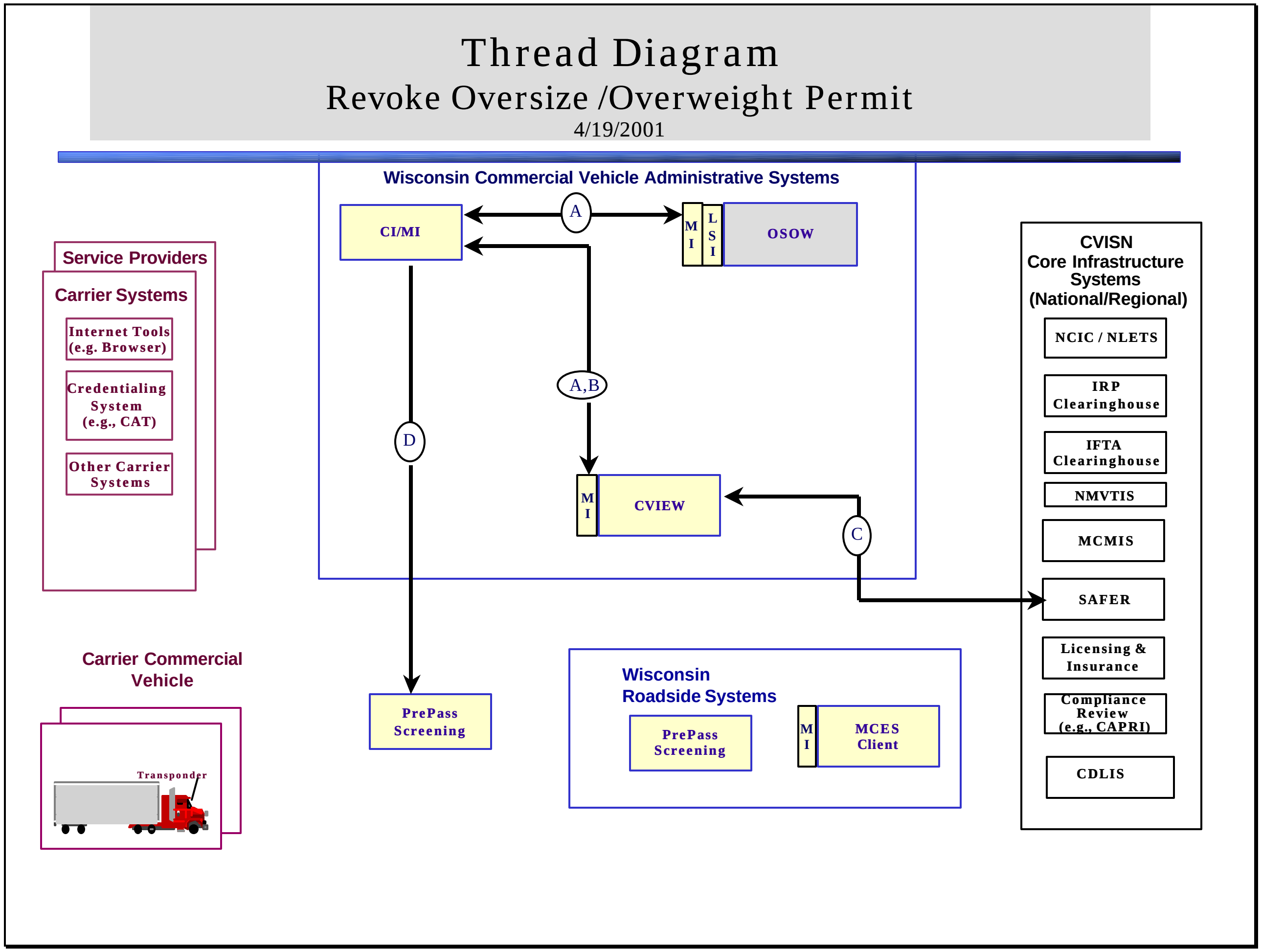
E. CVIEW formats query and sends to SAFER query mailbox using SMTP. (CVIEW is acting as the ASPEN in a SAFER - ASPEN Query (IR).

F. CVIEW retrieves response from the SAFER response mailbox employing the POP3 protocol.

G. CVIEW routes PIQ response to CI/MI.

H. CI/MI routes PIQ response back to MCES Client.

Revoke Oversize/Overweight Permit



Thread Diagram

Revoke Oversize /Overweight Permit

4/19/2001

Wisconsin Commercial Vehicle Administrative Systems
CI/MI
A
M I
L S I
OSOW
A,B
D
M I
CVIEW
C
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
CVISN Core Infrastructure Systems (National/Regional)
NCIC / NLETS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
CDLIS
Carrier Commercial Vehicle
Transponder
PrePass Screening
Wisconsin Roadside Systems
PrePass Screening
M I
MCES Client

Scenario Description
Revoke Oversize/Overweight Permit

A. OSOWupdates CVIEW with revocation information via the CI/MI.

B. CVIEW routes updated snapshot to CI/MI.

C. CVIEW updates SAFER at scheduled intervals.

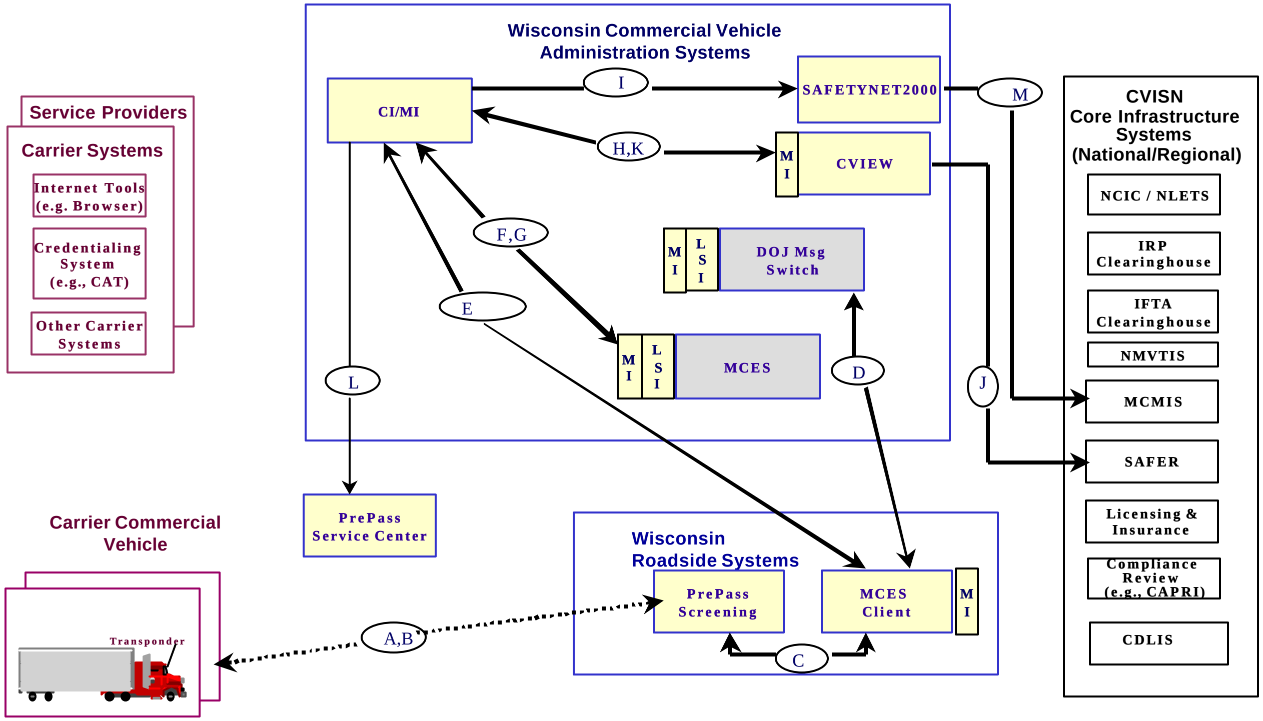
D. CI/MI periodically routes updated credential status to PrePass.

Screen Vehicles / Record Inspections & Report to SAFER

Thread Diagram

Screen Vehicles / Record Inspections & Report to SAFER

11/16/2001



Wisconsin Commercial Vehicle Administration Systems

CI/MI

SAFETYNET2000

MI CVIEW

MI LSI DOJ Msg Switch

MI LSI MCES

I

H,K

F,G

E

L

D

J

M

Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

CVISN Core Infrastructure Systems (National/Regional)

NCIC / NLETS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

CDLIS

Carrier Commercial Vehicle

Transponder

PrePass Service Center

A,B

Wisconsin Roadside Systems

PrePass Screening

MCES Client

MI

C

Scenario Description
Screen Vehicles / Record Inspections & Report to SAFER

A. **Select carrier vehicles to inspect. (PrePass Screening queries carrier vehicle tag).**

B. **PrePass Screening sends bypass or pull in signal to carrier vehicle tag.**

C. **PrePass Screening sends VIN # to MCES Client. (This is an expected future capability that will enable the MCES Client to access source systems for detail without manual entry.)**

D. **Determine level of inspection to conduct. MCES Client sends queries to state source systems via 3270 emulation capability.**

1. **Conduct inspection.**

E. **Inspection results entered into MCES Client which sends inspection update package to CI/MI.**

F. **CI/MI runs transaction specific script to route package to MCES.**

G. **MCES updates its database, creates snapshot update package and sends it to CI/MI.**

H. **CI/MI forwards snapshot update package & inspection report to CVIEW.**

I. **CI/MI forwards inspection report to SAFETYNET2000.**

J. **CVIEW forwards snapshot updates & inspection report to SAFER.**

K. **CVIEW forwards snapshot update to CI/MI for routing to PrePass Preview.**

L. **CI/MI periodically routes snapshot updates to PrePass PreView.**

Scenario Description

Screen Vehicles / Record Inspections & Report to SAFER

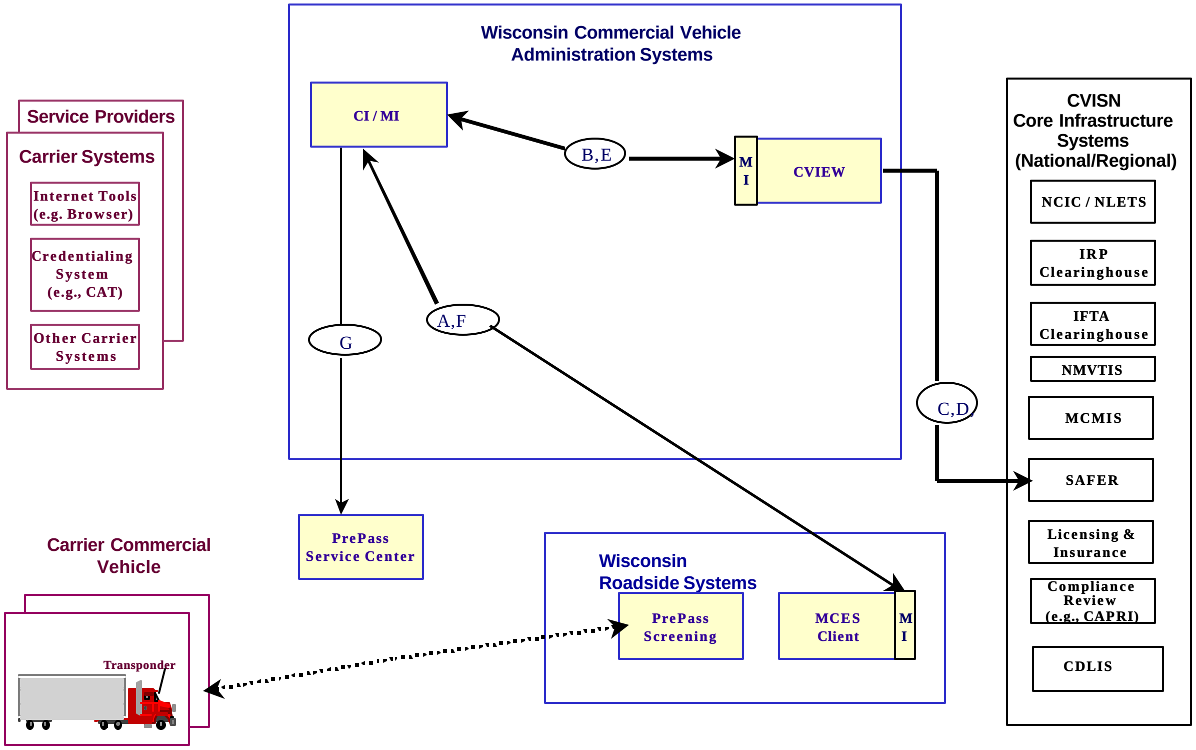
M. **SAFETYNET2000 forwards inspection report to MCMIS after state patrol editing is completed.**

Query for a Snapshot

Thread Diagram

Query for a Snapshot

11/16/2001



Wisconsin Commercial Vehicle Administration Systems
CI / MI
B,E
M I
CVIEW
A,F
G
C,D
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
CVISN Core Infrastructure Systems (National/Regional)
NCIC / NLETS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
CDLIS
Carrier Commercial Vehicle
Transponder
PrePass Service Center
Wisconsin Roadside Systems
PrePass Screening
MCES Client
M I

Scenario Description
Query for a Snapshot

A. MCES Client routes snapshot query to CI/MI supplying USDOT # as key.

B. CI/MI uses transaction specific script to route query to CVIEW.

C. CVIEW formats query and sends to SAFER query mailbox using SMTP. (CVIEW is acting as the ASPEN in a SAFER - ASPEN Query).

D. CVIEW retrieves response from the SAFER response mailbox employing the POP3 protocol.

1. CVIEW updates its snapshot data base if record(s) returned from SAFER

E. CVIEW routes snapshot query response to CI/MI.

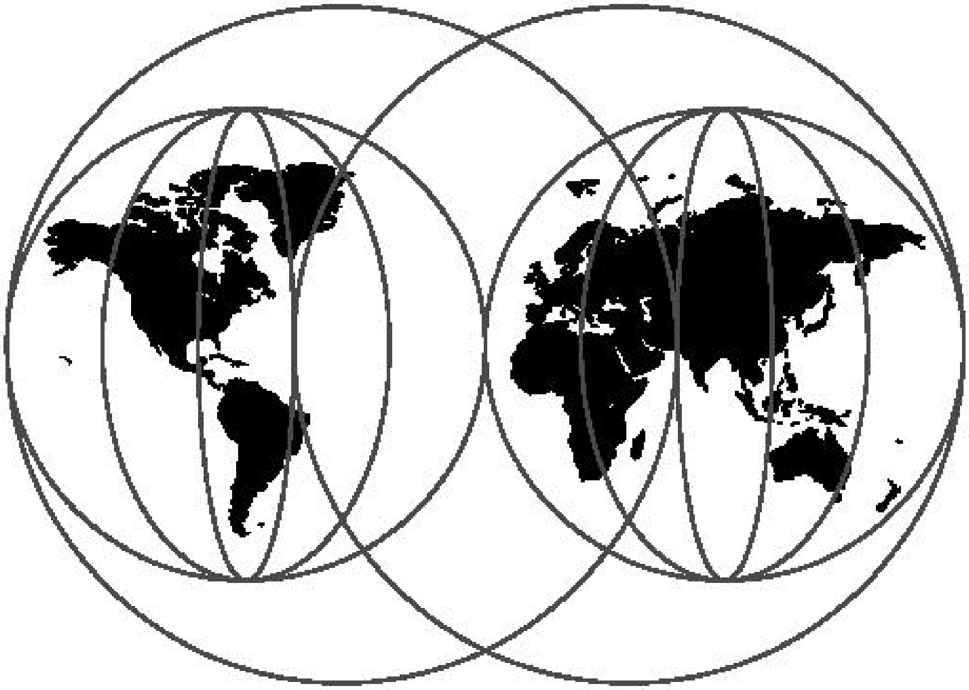
F. CI/MI routes snapshot response back to MCES Client.

G. CI/MI periodically routes snapshot updates to PrePass PreView.

Note: It is assumed the CVIEW keeps MCES Client databases in sync with its database. Thus, the snapshot query is checking the SAFER database only.

Appendix F – IBM MQSeries Primer

MQSeries Primer



MQSeries Enterprise Application Integration Center

Dieter Wackerow

MQSeries is IBM's award winning middleware for commercial messaging and queuing. It is used by thousands of customers in every major industry in many countries around the world. MQSeries speeds implementation of distributed applications by simplifying application development and test.

MQSeries runs on a variety of platforms. The MQSeries products enable programs to communicate with each other across a network of unlike components, such as processors, subsystems, operating systems and communication protocols. MQSeries programs use a consistent application program interface (API) across all platforms.

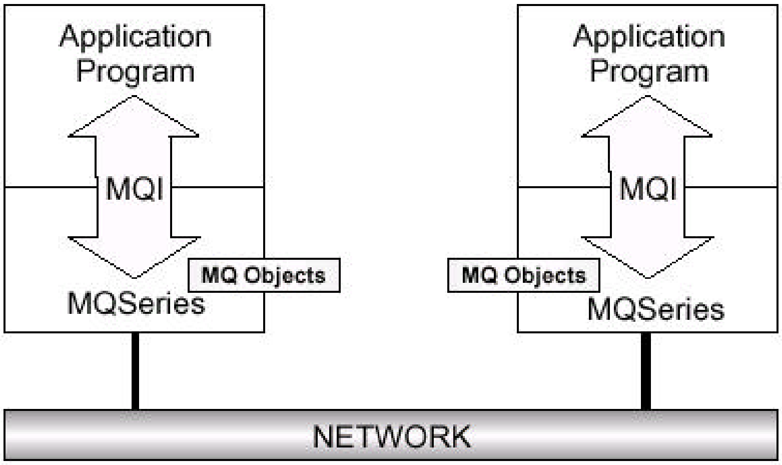


Figure 1. MQSeries at Run Time

Figure 1 shows the main parts of an MQSeries application at run time. Programs use MQSeries API calls, that is the Message Queue Interface (MQI), to communicate with a queue manager (MQM), the run-time program of MQSeries. For the queue manager to do its work, it refers to objects, such as queues and channels. The queue manager itself is an object as well.

The following provides a brief overview of MQSeries, including clients and servers.

What is Messaging and Queuing?

Message queuing is a method of program-to-program communication. Programs within an application communicate by writing and retrieving application-specific data (messages) to/from queues, without having a private, dedicated, logical connection to link them.

Messaging means that programs communicate with each other by sending data in messages and not by calling each other directly.

Queuing means that programs communicate through queues. Programs communicating through queues need not be executed concurrently.

With *asynchronous messaging*, the sending program proceeds with its own processing without waiting for a reply to its message. In contrast, *synchronous messaging* waits for the reply before it resumes processing. For the user, the underlying protocol is transparent. The user is concerned with conversational or data-entry type applications.

MQSeries is used in a client/server or distributed environment. Programs belonging to an application can run in one workstation or in different machines on different platforms. Applications can easily be moved from one system or platform to another. The programs can be written in various programming languages, including Java. The same queuing mechanism is valid for all platforms, and so are the currently 13 APIs.

Since MQSeries communicates via queues it can be referred to as using indirect program-to-program communication. The programmer cannot specify the name of the target application to which a message is sent. However, he or she can specify a target queue name; and each queue is associated with a program. An application can have one or more "input" queues and may have several "output" queues containing information for other servers to be processed, or for responses for the client that initiated the transaction.

The programmer does not have to worry about the target program being busy or not available. He or she isn't even concerned about the server being down or having no connection to it. The programmer sends messages to a queue that is associated with an application; and the application may or may not be available at the time of the request. MQSeries takes care of the transport to the target application and even starts it, if necessary.

If the target program is not available, the messages stay in a queue and get processed later. The queue is either in the sending machine or in the target machine, depending whether the connection between the two systems can be established or not. Applications can be running all day long or they can be triggered, that is, automatically started when a message arrives or after a specified number of messages have arrived.

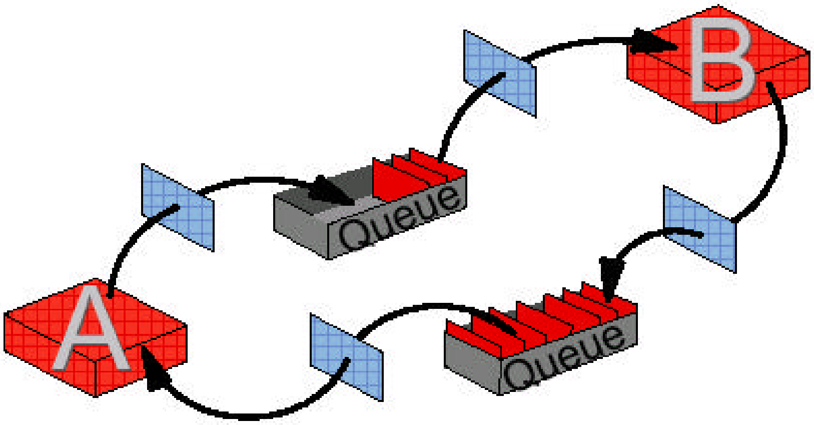


Figure 2. Messages and Queues

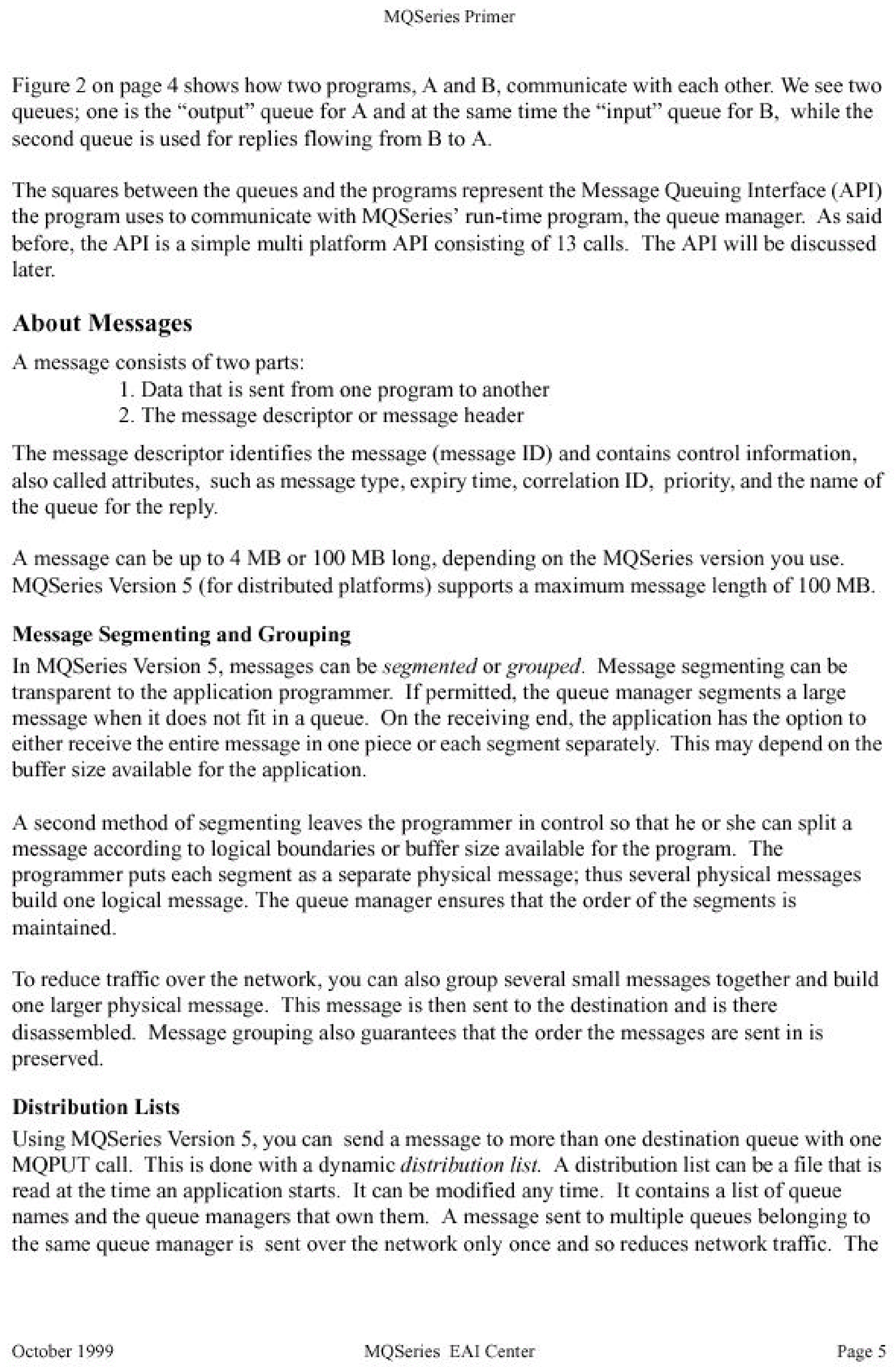


Figure 2 on page 4 shows how two programs, A and B, communicate with each other. We see two queues; one is the "output" queue for A and at the same time the "input" queue for B, while the second queue is used for replies flowing from B to A.

The squares between the queues and the programs represent the Message Queuing Interface (API) the program uses to communicate with MQSeries' run-time program, the queue manager. As said before, the API is a simple multi platform API consisting of 13 calls. The API will be discussed later.

About Messages

A message consists of two parts:

1. Data that is sent from one program to another
2. The message descriptor or message header

The message descriptor identifies the message (message ID) and contains control information, also called attributes, such as message type, expiry time, correlation ID, priority, and the name of the queue for the reply.

A message can be up to 4 MB or 100 MB long, depending on the MQSeries version you use. MQSeries Version 5 (for distributed platforms) supports a maximum message length of 100 MB.

Message Segmenting and Grouping

In MQSeries Version 5, messages can be *segmented* or *grouped*. Message segmenting can be transparent to the application programmer. If permitted, the queue manager segments a large message when it does not fit in a queue. On the receiving end, the application has the option to either receive the entire message in one piece or each segment separately. This may depend on the buffer size available for the application.

A second method of segmenting leaves the programmer in control so that he or she can split a message according to logical boundaries or buffer size available for the program. The programmer puts each segment as a separate physical message; thus several physical messages build one logical message. The queue manager ensures that the order of the segments is maintained.

To reduce traffic over the network, you can also group several small messages together and build one larger physical message. This message is then sent to the destination and is there disassembled. Message grouping also guarantees that the order the messages are sent in is preserved.

Distribution Lists

Using MQSeries Version 5, you can send a message to more than one destination queue with one MQPUT call. This is done with a dynamic *distribution list.* A distribution list can be a file that is read at the time an application starts. It can be modified any time. It contains a list of queue names and the queue managers that own them. A message sent to multiple queues belonging to the same queue manager is sent over the network only once and so reduces network traffic. The receiving queue manager replicates the messages and puts them into the destination queues. This function is called *late fan-out*.

Message Types

MQSeries knows four types of messages:

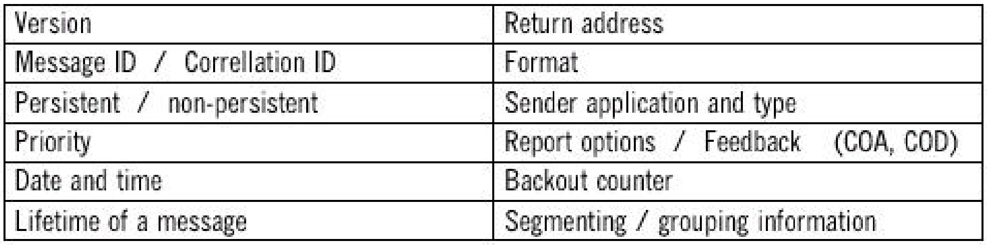
Datagram: A message containing information for which no response is expected.
Request: A message for which a reply is requested.
Reply: A reply to a request message.
Report: A message that describes an event such as the occurrence of an error or a confirmation on arrival or delivery.

Persistent and Non-Persistent Messages

Application design determines whether a message must reach its destination under any circumstances, or if it can be discarded when it cannot get there in time. MQSeries differentiates between *persistent* and *non-persistent* messages. *Delivery of persistent messages is assured*; they are written to logs to survive system failures. In an AS/400 these logs are Journal Receivers. Non-persistent messages cannot be recovered after a system restart.

The Message Descriptor

The table below contains some interesting attributes of the message descriptor. We mention them here because they explain some of the functions the queue manager provides for you.

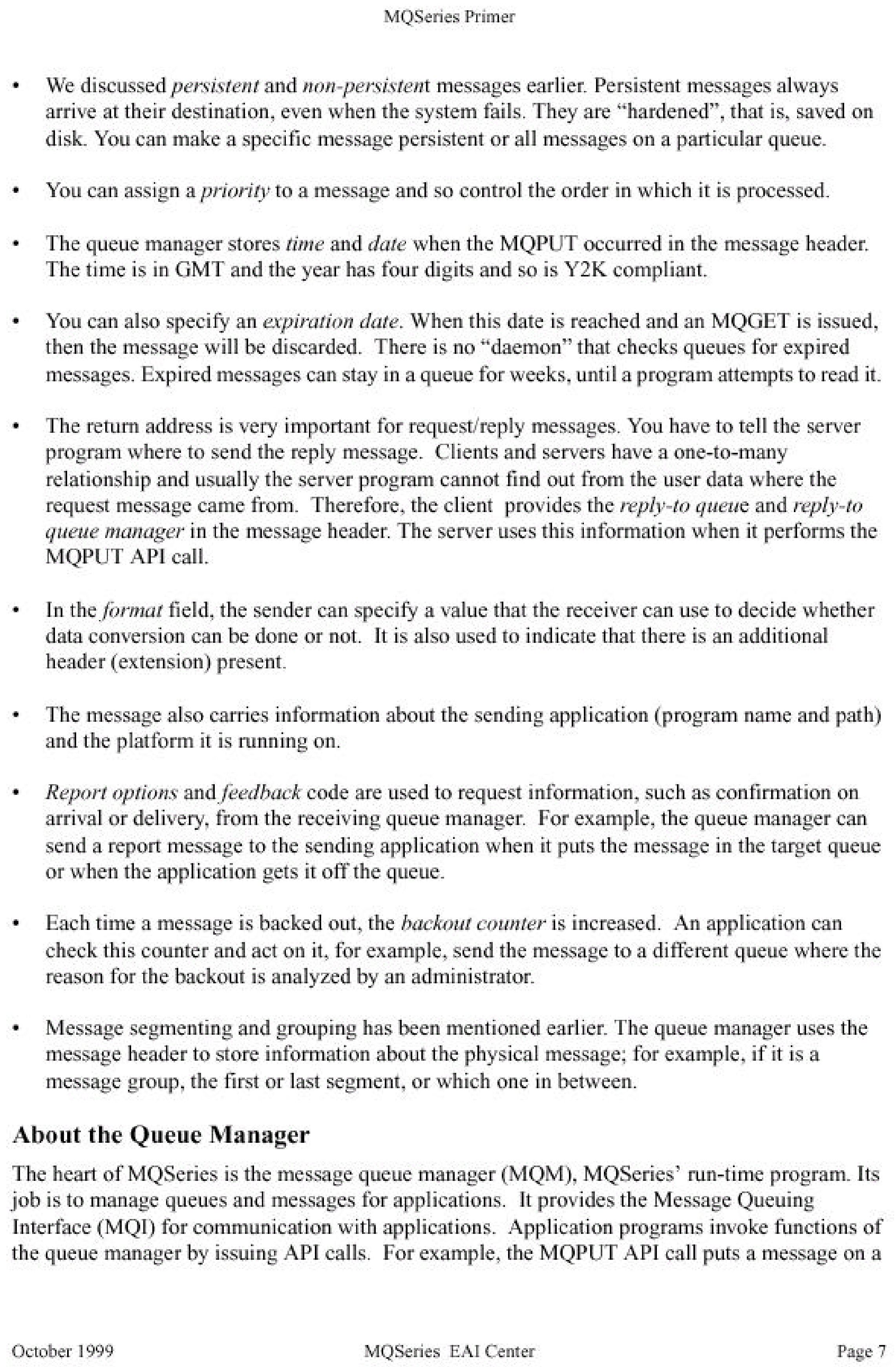


Version	Return address
Message ID / Correllation ID	Format
Persistent / non-persistent	Sender application and type
Priority	Report options / Feedback (COA, COD)
Date and time	Backout counter
Lifetime of a message	Segmenting / grouping information

Figure 3. Some Attributes of the Message Descriptor

- The *version* of the message descriptor depends on the MQSeries version and platform you use. For the functions introduced with Version 5 additional fields were needed to keep information about segments and their order and distribution list information, to name a few. This enlarged structure carries the version number 2. Other queue managers who don't support these functions ("Version 1 queue managers") treat the additional information as data.

- *Message* and/or *correlation ID* are used to identify a specific request or reply message. The programmer can move a value in one or both fields or have MQSeries create a unique ID for him or her. Before the programmer puts the request message in the queue he or she can save the ID(s) and use them in a subsequent get operation for the reply message. The program that receives the request message copies this information into the reply message. This allows the originating program (the one that gets the reply) to instruct MQSeries to look for a specific message in the queue instead of getting the first one in the queue.



- We discussed *persistent* and *non-persisten*t messages earlier. Persistent messages always arrive at their destination, even when the system fails. They are "hardened", that is, saved on disk. You can make a specific message persistent or all messages on a particular queue.

- You can assign a *priority* to a message and so control the order in which it is processed.

- The queue manager stores *time* and *date* when the MQPUT occurred in the message header. The time is in GMT and the year has four digits and so is Y2K compliant.

- You can also specify an *expiration date*. When this date is reached and an MQGET is issued, then the message will be discarded. There is no "daemon" that checks queues for expired messages. Expired messages can stay in a queue for weeks, until a program attempts to read it.

- The return address is very important for request/reply messages. You have to tell the server program where to send the reply message. Clients and servers have a one-to-many relationship and usually the server program cannot find out from the user data where the request message came from. Therefore, the client provides the *reply-to queu*e and *reply-to queue manager* in the message header. The server uses this information when it performs the MQPUT API call.

- In the *format* field, the sender can specify a value that the receiver can use to decide whether data conversion can be done or not. It is also used to indicate that there is an additional header (extension) present.

- The message also carries information about the sending application (program name and path) and the platform it is running on.

- *Report options* and *feedback* code are used to request information, such as confirmation on arrival or delivery, from the receiving queue manager. For example, the queue manager can send a report message to the sending application when it puts the message in the target queue or when the application gets it off the queue.

- Each time a message is backed out, the *backout counter* is increased. An application can check this counter and act on it, for example, send the message to a different queue where the reason for the backout is analyzed by an administrator.

- Message segmenting and grouping has been mentioned earlier. The queue manager uses the message header to store information about the physical message; for example, if it is a message group, the first or last segment, or which one in between.

About the Queue Manager

The heart of MQSeries is the message queue manager (MQM), MQSeries' run-time program. Its job is to manage queues and messages for applications. It provides the Message Queuing Interface (MQI) for communication with applications. Application programs invoke functions of the queue manager by issuing API calls. For example, the MQPUT API call puts a message on a queue to be read by another program using the MQGET API call. This scenario is shown in Figure 4.

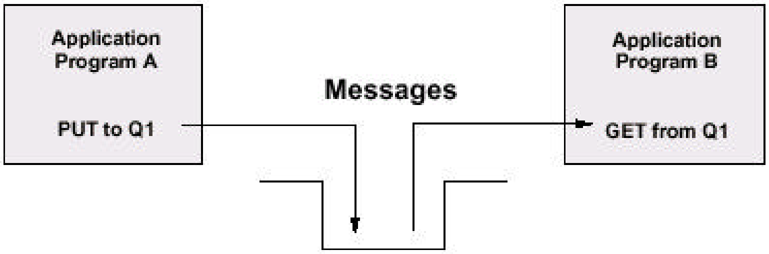


Figure 4. Program-to-Program Communication - One System

A program may send messages to another program that runs in the same machine as the queue manager (shown above), or to a program that runs in a remote system, such as a server or a host. The remote system has its own queue manager with its own queues. This scenario is shown in Figure 5.

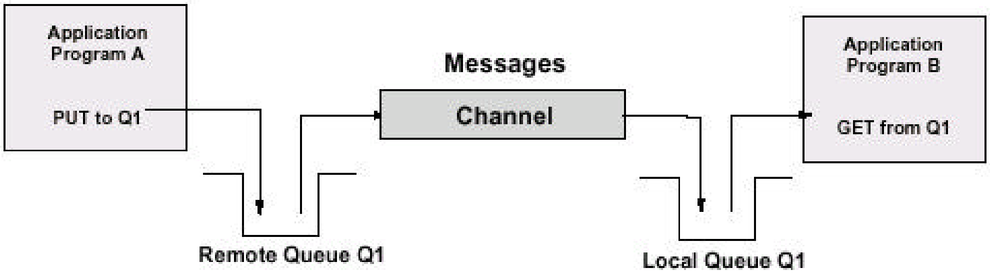


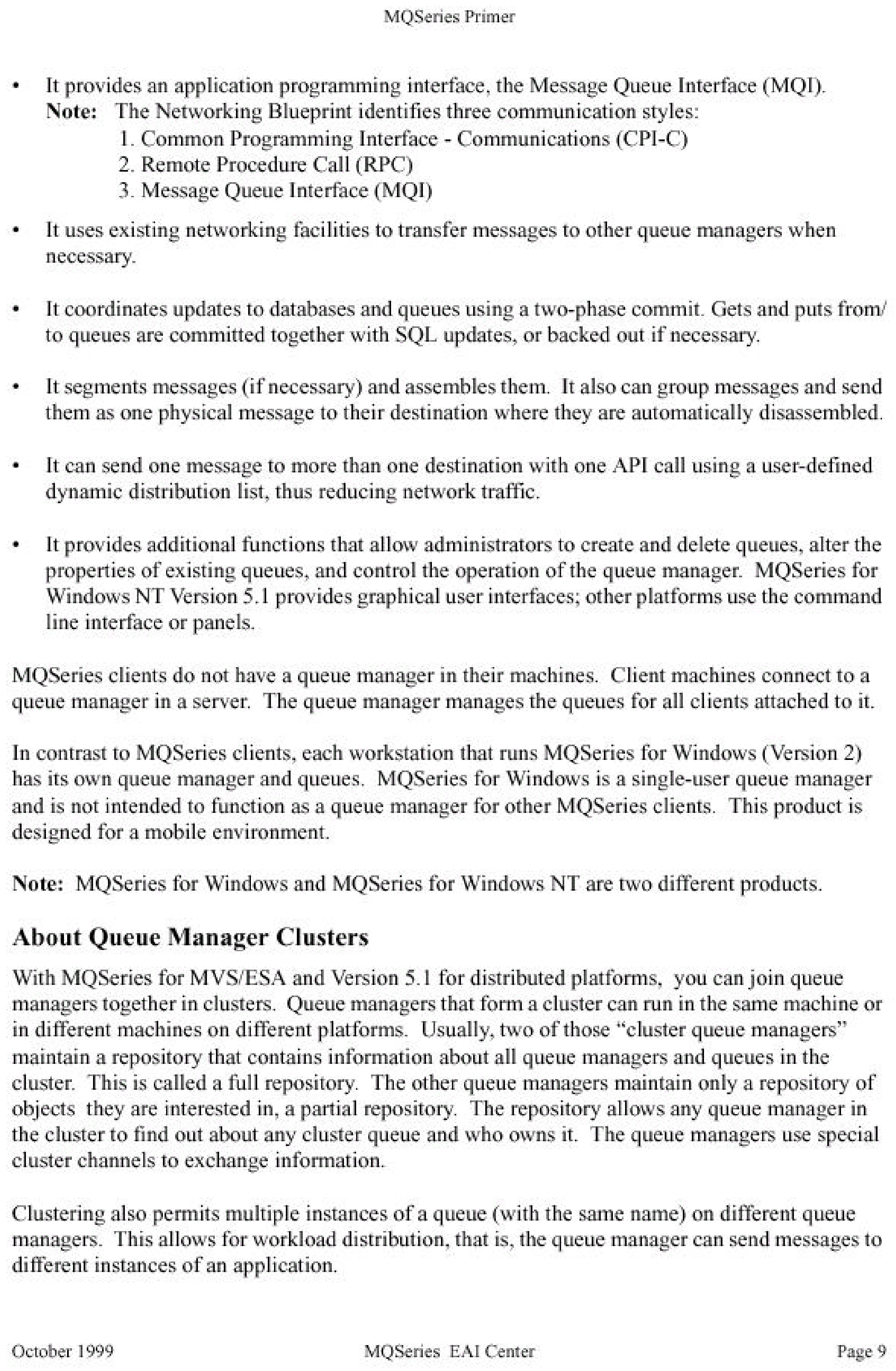
Figure 5. Program-to-Program Communication - Two Systems

The queue manager transfers messages to other queue managers via *channels* using existing network facilities, such as TCP/IP, SNA or SPX. Multiple queue managers can reside in the same machine. They also need channels to communicate.

Application programmers do not need to know where the program to which they are sending messages runs. They put their messages on a queue and let the queue manager worry about the destination machine and how to get the messages there. MQSeries knows what to do when the remote system is not available or the target program is not running or busy.

For the queue manager to do its work, it refers to objects that are defined by an administrator, usually when the queue manager is created or when a new application is added. The objects are described in "About Queue Manager Objects" on page 11. The functions of a queue manager can be summarized as follows:

- It manages queues of messages for application programs.



- It provides an application programming interface, the Message Queue Interface (MQI).
  Note: The Networking Blueprint identifies three communication styles:
  1. Common Programming Interface - Communications (CPI-C)
  2. Remote Procedure Call (RPC)
  3. Message Queue Interface (MQI)
- It uses existing networking facilities to transfer messages to other queue managers when necessary.
- It coordinates updates to databases and queues using a two-phase commit. Gets and puts from/ to queues are committed together with SQL updates, or backed out if necessary.
- It segments messages (if necessary) and assembles them. It also can group messages and send them as one physical message to their destination where they are automatically disassembled.
- It can send one message to more than one destination with one API call using a user-defined dynamic distribution list, thus reducing network traffic.
- It provides additional functions that allow administrators to create and delete queues, alter the properties of existing queues, and control the operation of the queue manager. MQSeries for Windows NT Version 5.1 provides graphical user interfaces; other platforms use the command line interface or panels.

MQSeries clients do not have a queue manager in their machines. Client machines connect to a queue manager in a server. The queue manager manages the queues for all clients attached to it.

In contrast to MQSeries clients, each workstation that runs MQSeries for Windows (Version 2) has its own queue manager and queues. MQSeries for Windows is a single-user queue manager and is not intended to function as a queue manager for other MQSeries clients. This product is designed for a mobile environment.

Note: MQSeries for Windows and MQSeries for Windows NT are two different products.

About Queue Manager Clusters

With MQSeries for MVS/ESA and Version 5.1 for distributed platforms, you can join queue managers together in clusters. Queue managers that form a cluster can run in the same machine or in different machines on different platforms. Usually, two of those “cluster queue managers” maintain a repository that contains information about all queue managers and queues in the cluster. This is called a full repository. The other queue managers maintain only a repository of objects they are interested in, a partial repository. The repository allows any queue manager in the cluster to find out about any cluster queue and who owns it. The queue managers use special cluster channels to exchange information.

Clustering also permits multiple instances of a queue (with the same name) on different queue managers. This allows for workload distribution, that is, the queue manager can send messages to different instances of an application.

In normal distributed processing, we send messages to a specific queue owned by a specific queue manager. All messages destined for that queue manager are placed in a transmission queue on the sender's side. This transmission queue has the same name as the destination queue manager. The message channel agents move the messages across the network and place them into the destination queues. Figure 6 shows the relationship between a transmission (Xmit) queue and the target queue manager.

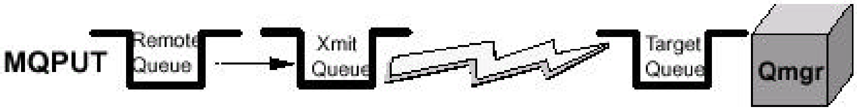


Figure 6. MQPUT to a Remote Queue

With clustering, you send a message to a queue with a specific name somewhere in the cluster, in Figure 7 represented by a cloud. You specify the name of a target queue, not the name of a remote queue definition. Clustering does not require remote queue definitions. They are only useful when you send a message to a queue manager that is not a member of the cluster. You can also specify a queue manager and direct the message to a specific queue, but very often it is left to the queue manager to determine where the queue is (or the queues are) and to which one to send the message.

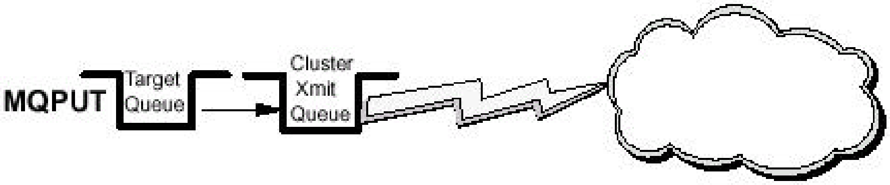


Figure 7. MQPUT to a Cluster Queue

The vision of an MQSeries cluster is as the place where multiple instances of a queue can exist. They come and go as an administrator requires in order to satisfy changing availability and throughput requirements. This has to be achieved completely dynamically and without placing the administrator under a great burden to configure and control. In addition, the programmer does not have to think about multiple queues; he or she just treats them as if writing to a single queue.

This is not to say that there is no burden on the programmer or administrator. Enhanced levels of availability and exploitation of parallelism do require some planning. The administrator or system designer must ensure that there is enough redundancy in the configuration to meet their needs. The application designer must ensure that messages are capable of being processed in multiple places.

You create multiple instances of a queue by defining a queue with the same name on multiple queue managers that belong to the cluster. You must also name the cluster when you define the queue. Without this attribute the queue would only be known locally. When the application specifies only the queue name, where is the message sent?

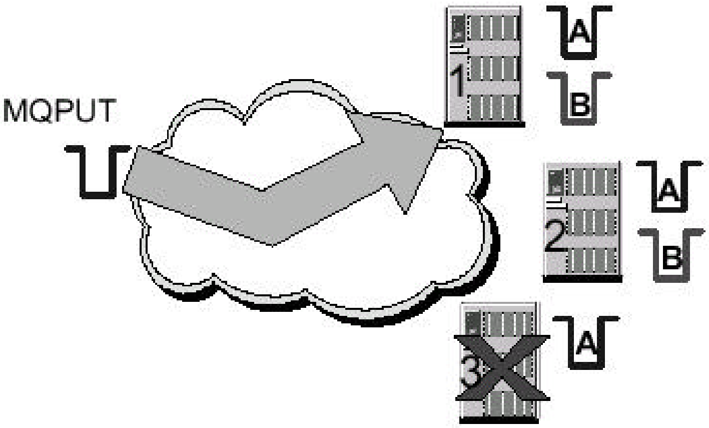


Figure 8. Accessing Cluster Queues

Figure 8 gives you an idea. MQSeries distributes the messages round-robin. You can, however, change this default action by writing your own workload balancing exit routine.

Figure 8 shows messages put in one of the three cluster queues named A. Each of the three queue managers on the right owns a queue with this name. By default, the first message is placed in queue A on queue manager 1, the next in queue A on queue manager 2, the third goes to queue manager 3 and the fourth message to the queue on queue manager 1 again.

In another scenario involving queue B, we notice that the third queue manager is down and the third instance of queue B is not available. The sending queue manager becomes aware of this problem because it subscribed to information about all queue manager and queues it is interested in, that is, where it sends messages. As soon as it finds out that there is a problem with the third instance of B, it distributes messages to the first two instances only. Special messages about changes of the status of cluster objects are instantly published to all queue managers that subscribed to that object.

About Queue Manager Objects

This section introduces you to queue manager objects, such as queues and channels. The queue manager itself is an object, too. Usually, an administrator creates one or more queue managers and their objects. A queue manager can use objects of the following types:

1. Queues
2. Process definitions
3. Channels

The objects are common across different MQSeries platforms. There are other objects that apply to MVS systems only, such as the buffer pool, PSID, and storage class. AS/400 MQ objects are known to the OS/400 operating system as object type *USRSPC (user space) in the QMQMDATA library.

Queues

Message queues are used to store messages sent by programs. There are local queues that are owned by the local queue manager, and remote queues that belong to a different queue manager. Queues are described in more detail in the section "About Message Queues" on page 13.

Channels

A channel is a logical communication link. In MQSeries, there are two different kinds of channels:

1. *Message channels*
   A message channel connects two queue managers via message channel agents (MCAs). Such a channel is unidirectional. It comprises two message channel agents, a sender and a receiver, and a communication protocol. An MCA is a program that transfers messages from a transmission queue to a communication link, and from a communication link into the target queue. For bidirectional communication you have to define two channel pairs consisting of a sender and a receiver. Message channel agents are also referred to as movers.

2. *MQI channel*s
   A Message Queue Interface (MQI) channel connects an MQSeries client to a queue manager in its server machine. Clients don't have a queue manager of their own. An MQI channel is bidirectional.

Figure 9 shows both channels types. You see four machines, two clients connected to their server machine via MQI channels, and the server connected to another server or a host via two unidirectional message channels. Some channels can be defined automatically by MQSeries. There are different types of message channels, depending on how the session between the queue managers is initiated and for what purpose they are used.

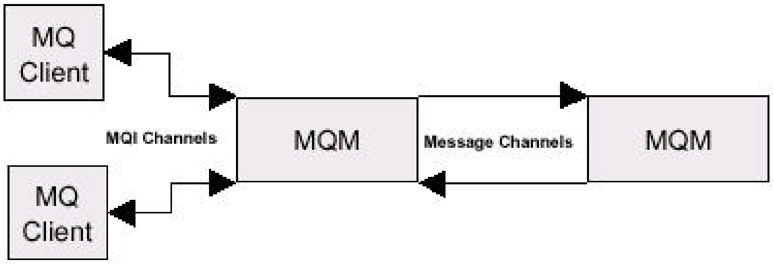


Figure 9. MQSeries Channels

To transmit non-persistent messages, a message channel can run at *two speeds*: fast and normal. Fast channels improve performance, but (non-persistent) messages can be lost in case of a channel failure.

A channel can use the following transport types: SNA LU 6.2, TCP/IP, NetBIOS, SPX and DEC Net. Not all are supported on all platforms.

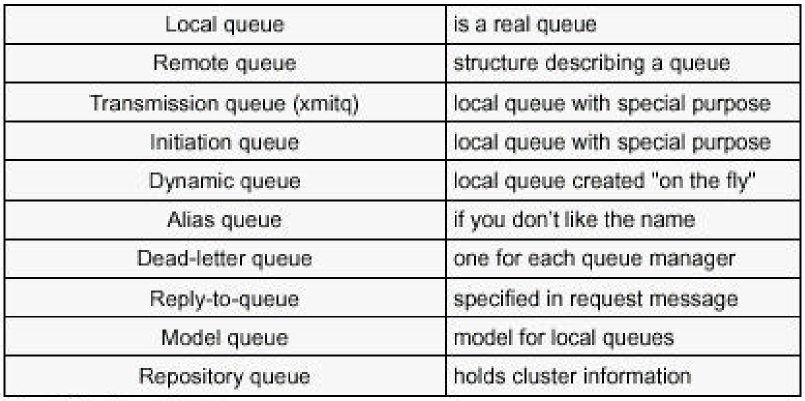
MQSeries for Windows Version 2 uses message channels to connect to other machines. Since this product is designed as a single user system, it does not support MQI channels. This product supports only TCP/IP.

Process Definitions

A process definition object defines an application to a queue manager. For example, it contains the name of the program (and its path) to be triggered when a message arrives for it.

About Message Queues

Queues are defined as objects belonging to a queue manager. MQSeries knows a number of different queue types, each with a specific purpose. The queues you use are located either in your machine and belong to the queue manager to which you are connected, or in your server (if you are a client). Figure 10 lists different queue types and their purposes. More detailed information is below.



Local queue	is a real queue
Remote queue	structure describing a queue
Transmission queue (xmitq)	local queue with special purpose
Initiation queue	local queue with special purpose
Dynamic queue	local queue created "on the fly"
Alias queue	if you don't like the name
Dead-letter queue	one for each queue manager
Reply-to-queue	specified in request message
Model queue	model for local queues
Repository queue	holds cluster information

Figure 10. Queue Types

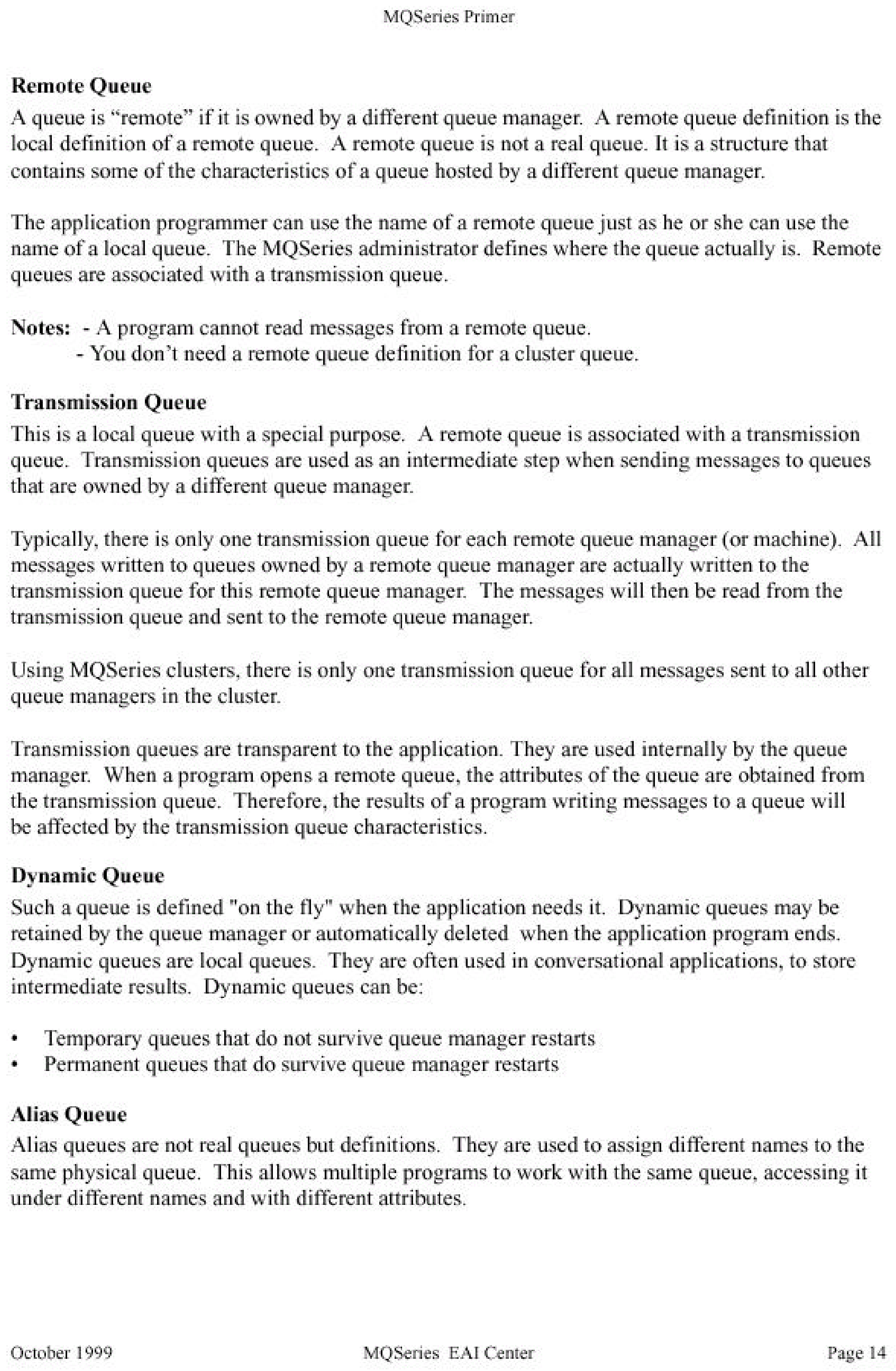
Local Queue

A queue is local if it is owned by the queue manager to which the application program is connected. It is used to store messages for programs that use the same queue manager. For example, program A and program B each has a queue for incoming messages and another queue for outgoing messages. Since the queue manager serves both programs, all four queues are local.

Note: Both programs do not have to run in the same workstation. Client workstations usually use a queue manager in a server machine.

Cluster Queue

A cluster queue is a local queue that is known throughout a cluster of queue managers, that is, any queue manager that belongs to the cluster can send messages to it without the need of a remote definition or defining channels to the queue manager that owns it.



Remote Queue

A queue is “remote” if it is owned by a different queue manager. A remote queue definition is the local definition of a remote queue. A remote queue is not a real queue. It is a structure that contains some of the characteristics of a queue hosted by a different queue manager.

The application programmer can use the name of a remote queue just as he or she can use the name of a local queue. The MQSeries administrator defines where the queue actually is. Remote queues are associated with a transmission queue.

Notes: - A program cannot read messages from a remote queue.
- You don’t need a remote queue definition for a cluster queue.

Transmission Queue

This is a local queue with a special purpose. A remote queue is associated with a transmission queue. Transmission queues are used as an intermediate step when sending messages to queues that are owned by a different queue manager.

Typically, there is only one transmission queue for each remote queue manager (or machine). All messages written to queues owned by a remote queue manager are actually written to the transmission queue for this remote queue manager. The messages will then be read from the transmission queue and sent to the remote queue manager.

Using MQSeries clusters, there is only one transmission queue for all messages sent to all other queue managers in the cluster.

Transmission queues are transparent to the application. They are used internally by the queue manager. When a program opens a remote queue, the attributes of the queue are obtained from the transmission queue. Therefore, the results of a program writing messages to a queue will be affected by the transmission queue characteristics.

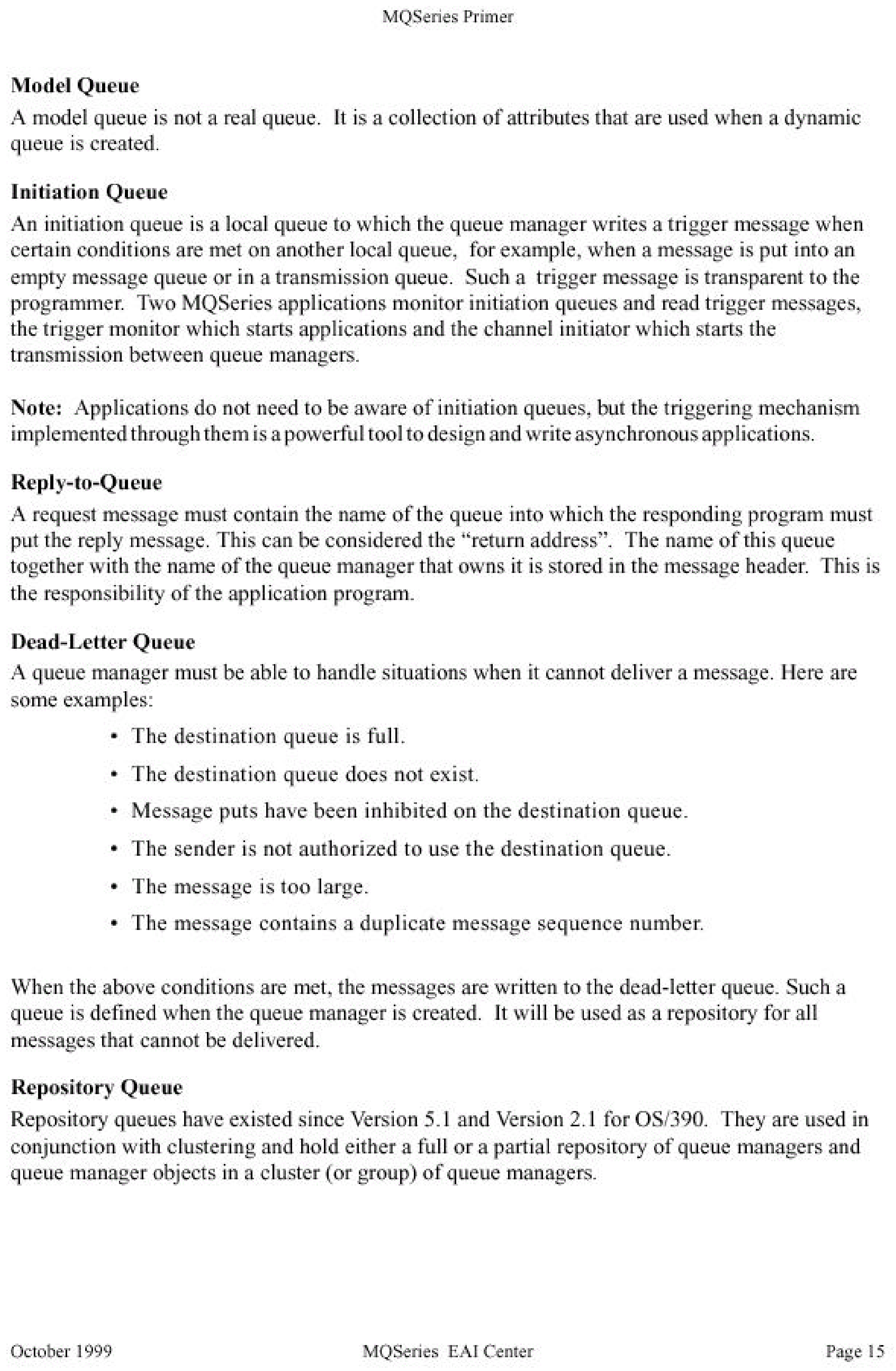
Dynamic Queue

Such a queue is defined "on the fly" when the application needs it. Dynamic queues may be retained by the queue manager or automatically deleted when the application program ends. Dynamic queues are local queues. They are often used in conversational applications, to store intermediate results. Dynamic queues can be:

- Temporary queues that do not survive queue manager restarts
- Permanent queues that do survive queue manager restarts

Alias Queue

Alias queues are not real queues but definitions. They are used to assign different names to the same physical queue. This allows multiple programs to work with the same queue, accessing it under different names and with different attributes.



Model Queue

A model queue is not a real queue. It is a collection of attributes that are used when a dynamic queue is created.

Initiation Queue

An initiation queue is a local queue to which the queue manager writes a trigger message when certain conditions are met on another local queue, for example, when a message is put into an empty message queue or in a transmission queue. Such a trigger message is transparent to the programmer. Two MQSeries applications monitor initiation queues and read trigger messages, the trigger monitor which starts applications and the channel initiator which starts the transmission between queue managers.

Note: Applications do not need to be aware of initiation queues, but the triggering mechanism implemented through them is a powerful tool to design and write asynchronous applications.

Reply-to-Queue

A request message must contain the name of the queue into which the responding program must put the reply message. This can be considered the "return address". The name of this queue together with the name of the queue manager that owns it is stored in the message header. This is the responsibility of the application program.

Dead-Letter Queue

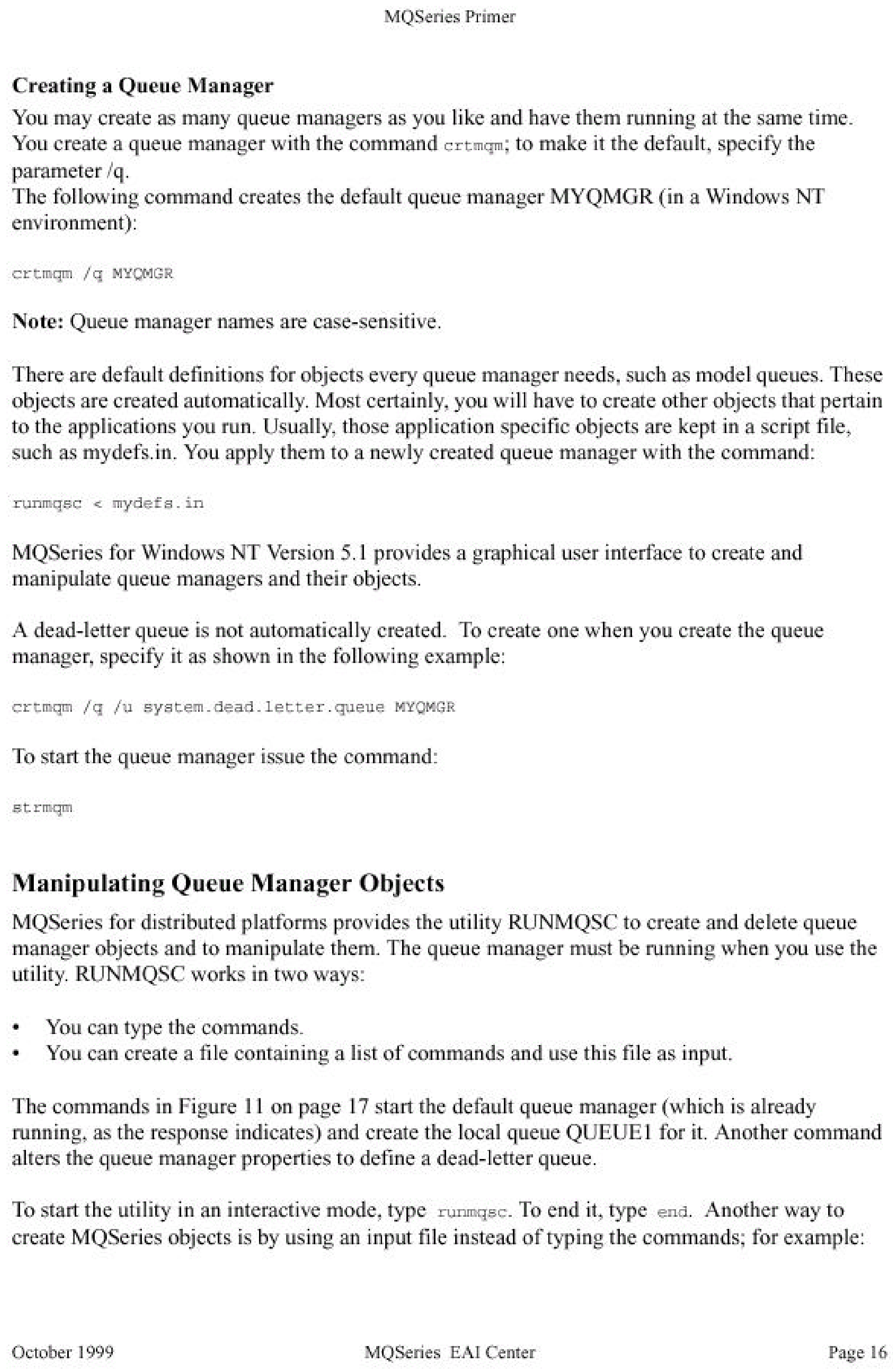
A queue manager must be able to handle situations when it cannot deliver a message. Here are some examples:

- The destination queue is full.
- The destination queue does not exist.
- Message puts have been inhibited on the destination queue.
- The sender is not authorized to use the destination queue.
- The message is too large.
- The message contains a duplicate message sequence number.

When the above conditions are met, the messages are written to the dead-letter queue. Such a queue is defined when the queue manager is created. It will be used as a repository for all messages that cannot be delivered.

Repository Queue

Repository queues have existed since Version 5.1 and Version 2.1 for OS/390. They are used in conjunction with clustering and hold either a full or a partial repository of queue managers and queue manager objects in a cluster (or group) of queue managers.



Creating a Queue Manager

You may create as many queue managers as you like and have them running at the same time. You create a queue manager with the command `crtmqm`; to make it the default, specify the parameter /q.
The following command creates the default queue manager MYQMGR (in a Windows NT environment):

```
crtmqm /q MYQMGR
```

Note: Queue manager names are case-sensitive.

There are default definitions for objects every queue manager needs, such as model queues. These objects are created automatically. Most certainly, you will have to create other objects that pertain to the applications you run. Usually, those application specific objects are kept in a script file, such as mydefs.in. You apply them to a newly created queue manager with the command:

```
runmqsc < mydefs.in
```

MQSeries for Windows NT Version 5.1 provides a graphical user interface to create and manipulate queue managers and their objects.

A dead-letter queue is not automatically created. To create one when you create the queue manager, specify it as shown in the following example:

```
crtmqm /q /u system.dead.letter.queue MYQMGR
```

To start the queue manager issue the command:

```
strmqm
```

Manipulating Queue Manager Objects

MQSeries for distributed platforms provides the utility RUNMQSC to create and delete queue manager objects and to manipulate them. The queue manager must be running when you use the utility. RUNMQSC works in two ways:

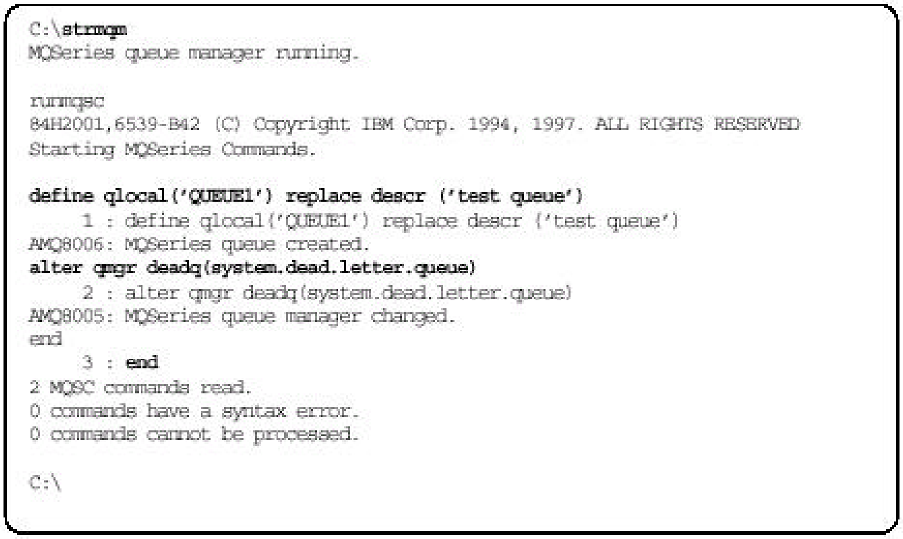
- You can type the commands.
- You can create a file containing a list of commands and use this file as input.

The commands in Figure 11 on page 17 start the default queue manager (which is already running, as the response indicates) and create the local queue QUEUE1 for it. Another command alters the queue manager properties to define a dead-letter queue.

To start the utility in an interactive mode, type `runmqsc`. To end it, type `end`. Another way to create MQSeries objects is by using an input file instead of typing the commands; for example:

```
runmqsc < mydefs.in > a.a
```

where mydefs.in is the script file that contains the commands and a.a is the file that will contain the responses from the RUNMQSC utility, so that you can check if any error occurred. The output can either appear in the window or can be redirected to a file.



```
C:\strmqm
MQSeries queue manager running.

runmqsc
84H2001,6539-B42 (C) Copyright IBM Corp. 1994, 1997. ALL RIGHTS RESERVED
Starting MQSeries Commands.

define qlocal('QUEUE1') replace descr ('test queue')
     1 : define qlocal('QUEUE1') replace descr ('test queue')
AMQ8006: MQSeries queue created.
alter qmgr deadq(system.dead.letter.queue)
     2 : alter qmgr deadq(system.dead.letter.queue)
AMQ8005: MQSeries queue manager changed.
end
     3 : end
2 MQSC commands read.
0 commands have a syntax error.
0 commands cannot be processed.

C:\
```

Figure 11. Manipulating Objects Using Control Commands

Clients and Servers

MQSeries distinguishes clients and servers. Before you install MQSeries on a distributed platform you have to decide if the workstation will be an MQSeries client, an MQSeries server, or both. With MQSeries for Windows a new term was introduced, the leaf node (described later). There are two kinds of clients:

- Slim client or MQSeries client
- Fat client

Fat clients have a local queue manager; slim clients don't.

When a slim client cannot connect to its server it cannot work, because the queue manager and queues for a slim client reside in the server. Usually, an MQSeries client is a slim client. Several of these clients share MQSeries objects, and the queue manager is one of them, in the server to which they are attached.

Note: The MQSeries Client for Java is a slim client.

In some cases it may be advantageous to have queues in the end user's workstation, especially in a mobile environment. That allows you to run your application when a connection between client and server does not (temporarily) exist.

You may install client and server software in the same system and use it as an end user's workstation. If your operating system is Windows NT you can install MQSeries for Windows NT V5.1 or MQSeries for Windows V2.1 (also called MQWin). If your operating system is Windows 95 use MQWin V2.1. This product has been designed for end users and uses fewer resources.

The difference between an end user's workstation that is a client and one that has a queue manager is the way messages are sent. The queues reside either in the end user's workstation or in the server.

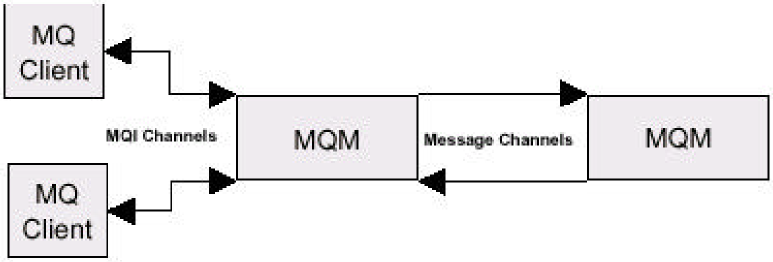


Figure 12. MQI and Message Channels

Figure 12 shows again the use of MQI and message channels.

- MQI channels connect clients to a queue manager in a server machine. All MQSeries objects for the client reside in the server. MQI channels are faster than message channels.

- A message channel connects a queue manager to another queue manager. The queue manager can reside in the same or in a different machine.

The following summarizes the three workstation types:

MQSeries Client

A client workstation does not have a queue manager of its own. It shares a queue manager in a server with other clients. All MQSeries objects, such as queues, are in the server. Since the connection between client and server is synchronous, the application cannot work when the communication is broken. You could refer to such workstations as "slim" clients.

MQSeries Server

A workstation can be a client and a server. A server is an intermediate node between other nodes. It serves clients that have no queue manager and manages the message flow between its clients, itself and other servers. In addition to the server software you may install the client software, too. This configuration is used in an application development environment.

Leaf Node

MQSeries for Windows was designed for use by a single user. It has its own "small footprint" queue manager with its own objects. However, it is not an intermediate node between other nodes. It is called a leaf node. You could also refer to it as a "fat" client. This product is able to queue outbound messages when connection to a server or host is not available, and inbound messages when the appropriate application is not active.

How MQSeries Works

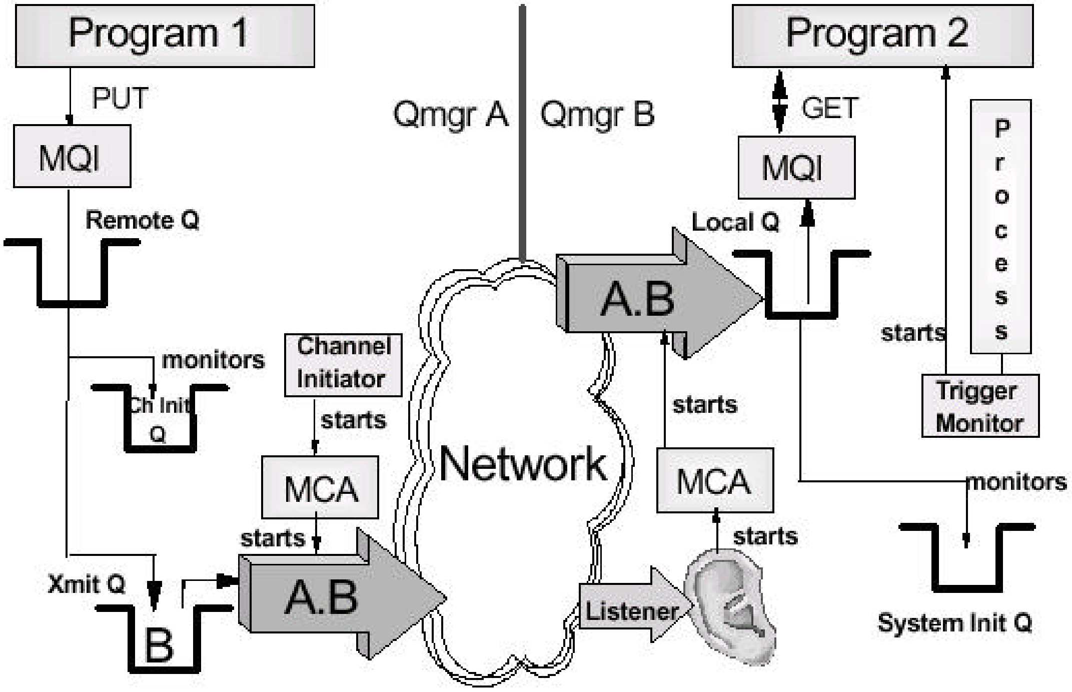


Figure 13. MQSeries - Parts and Logic

Figure 13 shows the parts and architecture of MQSeries. The application program uses the Message Queue Interface (MQI) to communicate with the queue manager. The MQI is described in more detail later. The queuing system consists of the following parts:

- Queue Manager (MQM)
- Listener
- Trigger Monitor
- Channel Initiator
- Message Channel Agent (MCA) or mover

When the application program wants to put a message on a queue it issues an MQPUT API call. This invokes the MQI. The queue manager checks whether the queue referenced in the MQPUT is local or remote. If it is a remote queue, the message is placed into the transmission (xmit) queue. The queue manager adds a header that contains information from the remote queue definition, such as destination queue manager name and destination queue name.

Note: Each remote queue must be associated with an xmit queue. Usually, all messages destined for one remote machine use the same xmit queue.

Transmission is done via channels. Channels can be started manually or automatically. To start a channel automatically, the xmit queue must be associated with a channel initiation queue. Figure 13 on page 19 shows that the queue manager puts a message into the xmit queue and another message into the channel initiation queue. This queue is monitored by the *channel initiator*.

The channel initiator is an MQSeries program that must be running in order to monitor initiation queues. When the channel initiator detects a message in the initiation queue, it starts the message channel agent (MCA) for the particular channel. This program moves the message over the network to the other machine, using the sender part of the unidirectional message channel pair.

On the receiving end, a *listener* program must have been started. The listener, also supplied with MQSeries, monitors a specified port, by default, the port dedicated to MQSeries, 1414. When a message arrives, it starts the *message channel agent*. The MCA moves the message into the specified local queue using the receiver part of the message channel pair.

Note: Both channel definitions, sender and receiver, must have the same name. For the reply, you need another message channel pair.

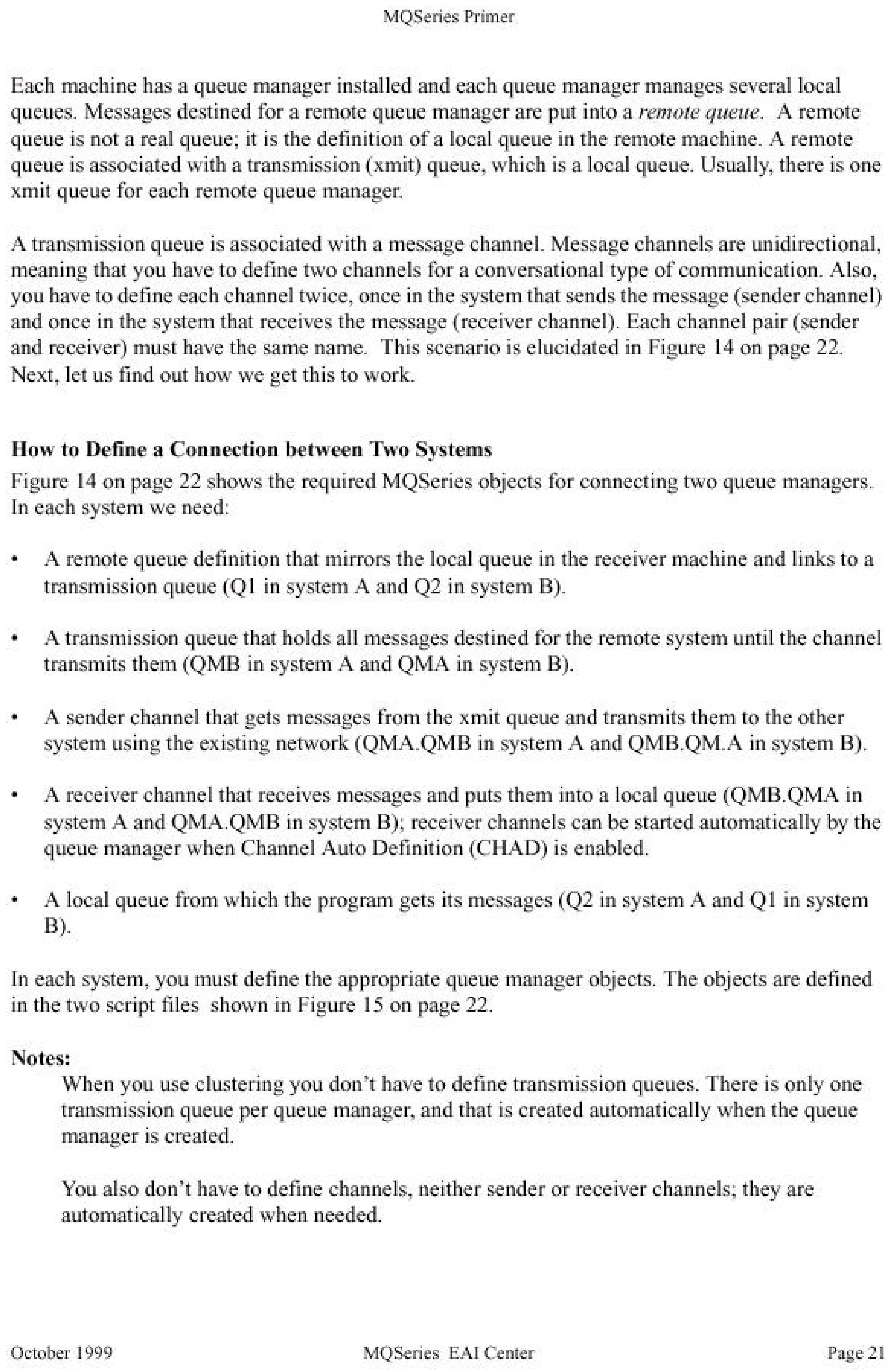
The program that processes the incoming message can be started manually or automatically. To start the program automatically, an initiation queue and a process must be associated with the local queue, and the *trigger monitor* must be running.

When the program starts automatically, the MCA puts the incoming message into the local queue and a trigger message into the initiation queue. This queue is monitored by the trigger monitor. This program invokes the application program specified in the process definition. The application issues an MQGET API call to retrieve the message from the local queue.

Communication between Queue Managers

In this section, we discuss what you have to define to send messages to a queue manager that resides in another system. We use message channels for communication between queue managers as shown in Figure 12 on page 18.

The logic is illustrated in Figure 14 on page 22 and the necessary MQSeries definitions are shown in Figure 15 on page 22.



Each machine has a queue manager installed and each queue manager manages several local queues. Messages destined for a remote queue manager are put into a *remote queue*. A remote queue is not a real queue; it is the definition of a local queue in the remote machine. A remote queue is associated with a transmission (xmit) queue, which is a local queue. Usually, there is one xmit queue for each remote queue manager.

A transmission queue is associated with a message channel. Message channels are unidirectional, meaning that you have to define two channels for a conversational type of communication. Also, you have to define each channel twice, once in the system that sends the message (sender channel) and once in the system that receives the message (receiver channel). Each channel pair (sender and receiver) must have the same name. This scenario is elucidated in Figure 14 on page 22. Next, let us find out how we get this to work.

How to Define a Connection between Two Systems

Figure 14 on page 22 shows the required MQSeries objects for connecting two queue managers. In each system we need:

- A remote queue definition that mirrors the local queue in the receiver machine and links to a transmission queue (Q1 in system A and Q2 in system B).
- A transmission queue that holds all messages destined for the remote system until the channel transmits them (QMB in system A and QMA in system B).
- A sender channel that gets messages from the xmit queue and transmits them to the other system using the existing network (QMA.QMB in system A and QMB.QM.A in system B).
- A receiver channel that receives messages and puts them into a local queue (QMB.QMA in system A and QMA.QMB in system B); receiver channels can be started automatically by the queue manager when Channel Auto Definition (CHAD) is enabled.
- A local queue from which the program gets its messages (Q2 in system A and Q1 in system B).

In each system, you must define the appropriate queue manager objects. The objects are defined in the two script files shown in Figure 15 on page 22.

Notes:

When you use clustering you don't have to define transmission queues. There is only one transmission queue per queue manager, and that is created automatically when the queue manager is created.

You also don't have to define channels, neither sender or receiver channels; they are automatically created when needed.

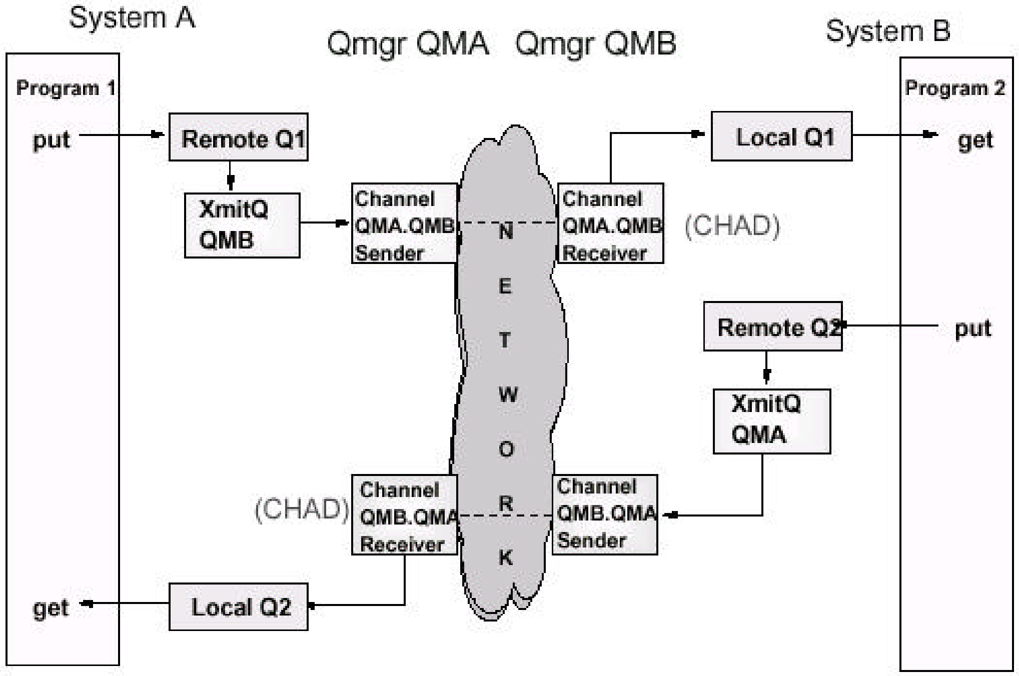
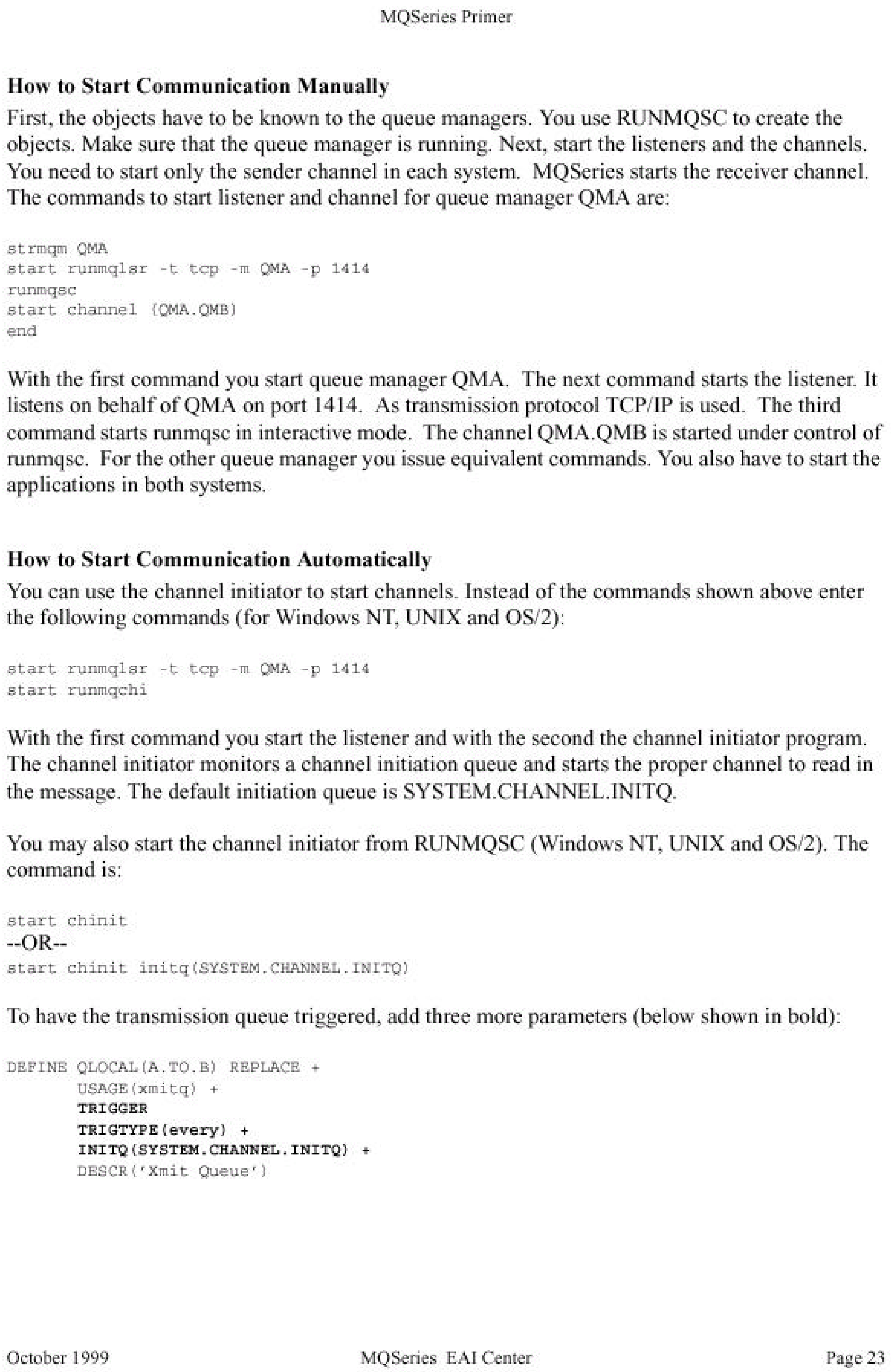


Figure 14. Communication between Two Queue Managers

System A (QMA)	System B (QMB)
DEFINE QREMOTE(Q1) + RNAME(Q1) RQMNAME(QMB) + XMITQ(QMB)	DEFINE QLOCAL(Q1)
DEFINE QLOCAL(QMB) + USAGE(xmitq)	
DEFINE CHANNEL(QMA.QMB) + CHLTYPE(sdr) + XMITQ(QMB) + TRPTYPE(tcp) + CONNAME(9.24.104.123)	DEFINE CHANNEL(QMA.QMB) + CHLTYPE(rcvr) + TRPTYPE(tcp)
DEFINE QLOCAL(Q2)	DEFINE QREMOTE(Q2) + RNAME(Q2) RQMNAME(QMA) + XMITQ(QMA)
	DEFINE QLOCAL(QMA) + USAGE(xmitq)
DEFINE CHANNEL(QMB.QMA) + CHLTYPE(rcvr) + TRPTYPE(tcp)	DEFINE CHANNEL(QMB.QMA) + CHLTYPE(sdr) + XMITQ(QMA) + TRPTYPE(tcp) CONNAME(ABC1)

Figure 15. MQSeries Objects Defining Connection between Two Queue Managers



How to Start Communication Manually

First, the objects have to be known to the queue managers. You use RUNMQSC to create the objects. Make sure that the queue manager is running. Next, start the listeners and the channels. You need to start only the sender channel in each system. MQSeries starts the receiver channel. The commands to start listener and channel for queue manager QMA are:

```
strmqm QMA
start runmqlsr -t tcp -m QMA -p 1414
runmqsc
start channel (QMA.QMB)
end
```

With the first command you start queue manager QMA. The next command starts the listener. It listens on behalf of QMA on port 1414. As transmission protocol TCP/IP is used. The third command starts runmqsc in interactive mode. The channel QMA.QMB is started under control of runmqsc. For the other queue manager you issue equivalent commands. You also have to start the applications in both systems.

How to Start Communication Automatically

You can use the channel initiator to start channels. Instead of the commands shown above enter the following commands (for Windows NT, UNIX and OS/2):

```
start runmqlsr -t tcp -m QMA -p 1414
start runmqchi
```

With the first command you start the listener and with the second the channel initiator program. The channel initiator monitors a channel initiation queue and starts the proper channel to read in the message. The default initiation queue is SYSTEM.CHANNEL.INITQ.

You may also start the channel initiator from RUNMQSC (Windows NT, UNIX and OS/2). The command is:

```
start chinit
```

--OR--

```
start chinit initq(SYSTEM.CHANNEL.INITQ)
```

To have the transmission queue triggered, add three more parameters (below shown in bold):

```
DEFINE QLOCAL(A.TO.B) REPLACE +
       USAGE(xmitq) +
       TRIGGER
       TRIGTYPE(every) +
       INITQ(SYSTEM.CHANNEL.INITQ) +
       DESCR('Xmit Queue')
```

The queue manager can trigger the process that starts the channel program in three ways:

- When the first message is put into the transmission queue
- Every time a message is put into the xmit queue
- When the queue contains a specified number of messages

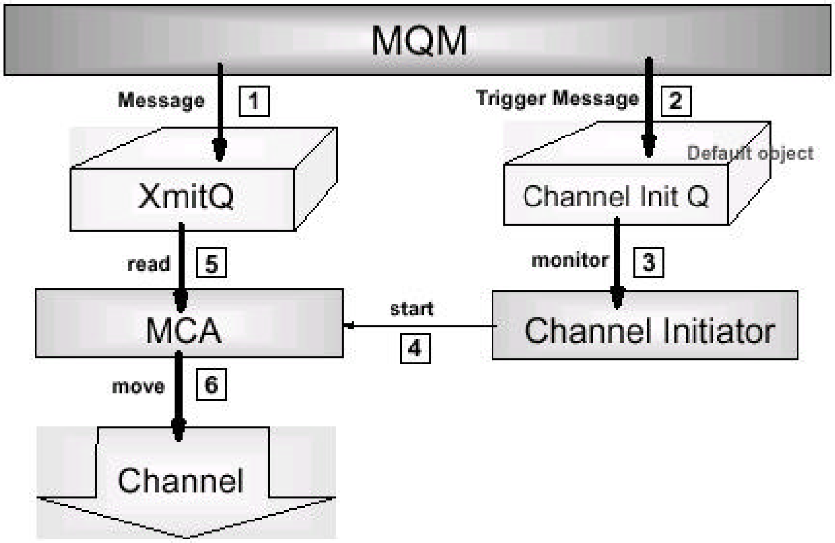


Figure 16. Triggering Channels

Figure 16 shows the logic behind triggering:

1. The program issues an MQPUT to a remote queue and a message is placed into the transmission queue.

2. When the queue manager puts a message into the transmission queue, it checks the trigger type specified in the queue definition. Depending on that definition and on how many messages are in the queue, it may put an additional message in the channel initiation queue. This "trigger message" is transparent to the user.

3. Since the channel initiator was started earlier, for example, at boot time, it monitors the channel initiation queue and removes the trigger message.

4. The channel initiator starts the message channel agent (also called mover).

5. The channel program gets the message off the transmission queue and invokes any channel exit routines, if specified.

6. The message is then moved over the network to its destination.

How to Trigger Applications

This section describes how to trigger an application program that runs in the server machine. Both triggering and triggered applications can run under the same or different queue managers.

Note: MQSeries for Windows V2.1 does not support triggering.

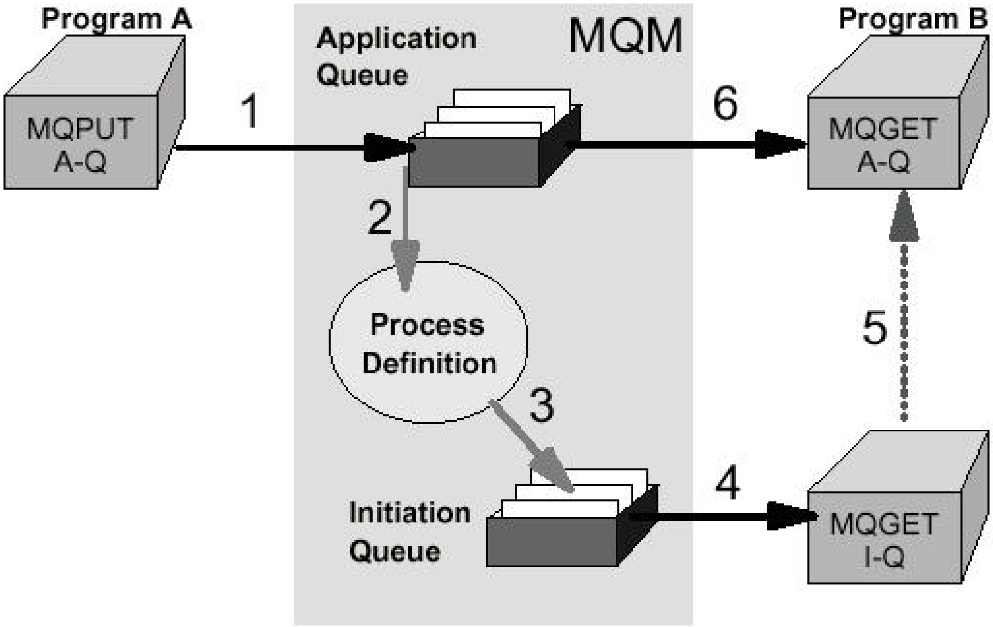


Figure 17. Triggering an Application

Figure 17 shows the logic of triggering. Here Program A sends a message to A-Q to be processed by Program B. The MQSeries triggering mechanism is as follows:

1. Program A issues an MQPUT and puts a message into A-Q for Program B.
2. The queue manager processes this API call and puts the message into the application queue.
3. It also finds out that the queue is triggered. It creates a trigger message and looks in the Process Definition to find the name of the application and puts it in the trigger message. The trigger message is put into the initiation queue.
4. The trigger monitor gets the trigger message from the initiation queue and starts the program specified.
5. The application program starts running and issues an MQGET to retrieve the message from the application queue.

The definitions necessary to trigger an application are as follows:

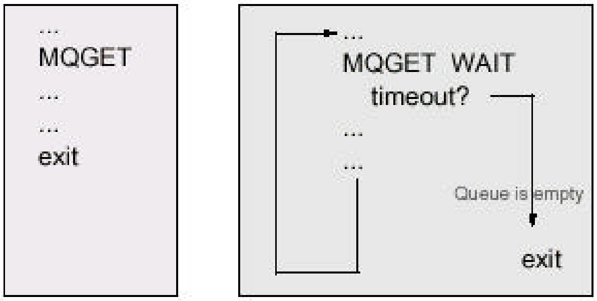
- The target queue must have “triggering” specified as shown in bold below:

```
DEFINE QLOCAL(A-Q)  REPLACE +
        TRIGGER
        TRIGTYPE(first) +
        INITQ(SYSTEM.DEFAULT.INITIATION.QUEUE ) +
        PROCESS(proc1)
        DESCR('This is a triggered queue')
```

- The process definition associated with the target queue can be this:

```
DEFINE PROCESS(proc1)  REPLACE +
        DESCR('Process to start server program') +
        APPLTYPE(WINDOWSNT) +
        APPPLICID('c:\test\myprog.exe')
```

What trigger type to use depends on how the application is written. You have three choices:



- EVERY Every time a message is put in the target queue a trigger message is also put in the initiation queue. Use this when your program exits after processing one message or transaction, as shown above on the left.

- FIRST A trigger message is put in the initiation queue only when the target queue has been empty. Use this when the program exits only then when there are no more messages in the queue, as shown on the right.

- n messages A trigger message is put in the initiation queue when there are n messages in the target queue. For example, you can start a batch program when the queue holds 1000 messages.

Communication between Client and Server

Below we discuss what you have to do to define and test the connection between an MQ client and its MQ server. A more detailed description is provided in the publication *MQSeries Clients* , GC33-1632.

How to Define a Client/Server Connection

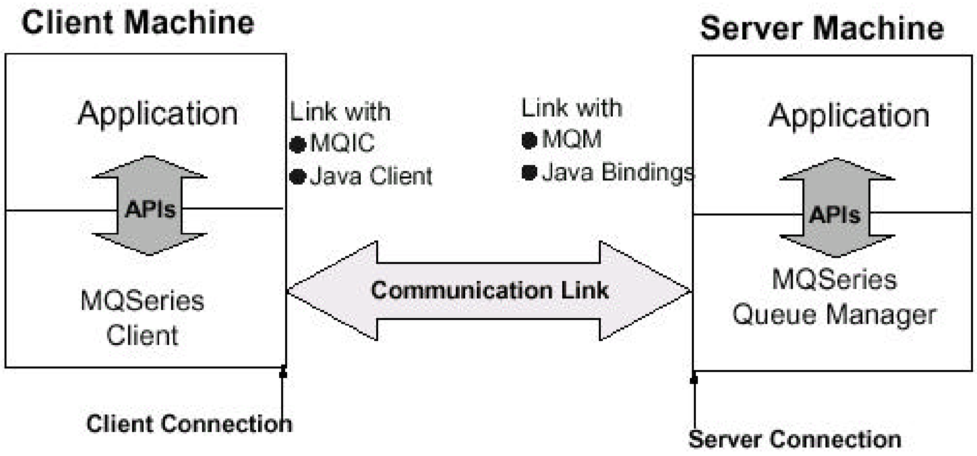


Figure 18. Client/Server Connection

Figure 18 shows that the MQSeries Client product is installed in the client machine. We said before that clients and servers are connected with MQI channels. An MQI channel consists of a sender/receiver pair, called Client Connection (CLNTCONN) and Server Connection (SVCONN) channel.

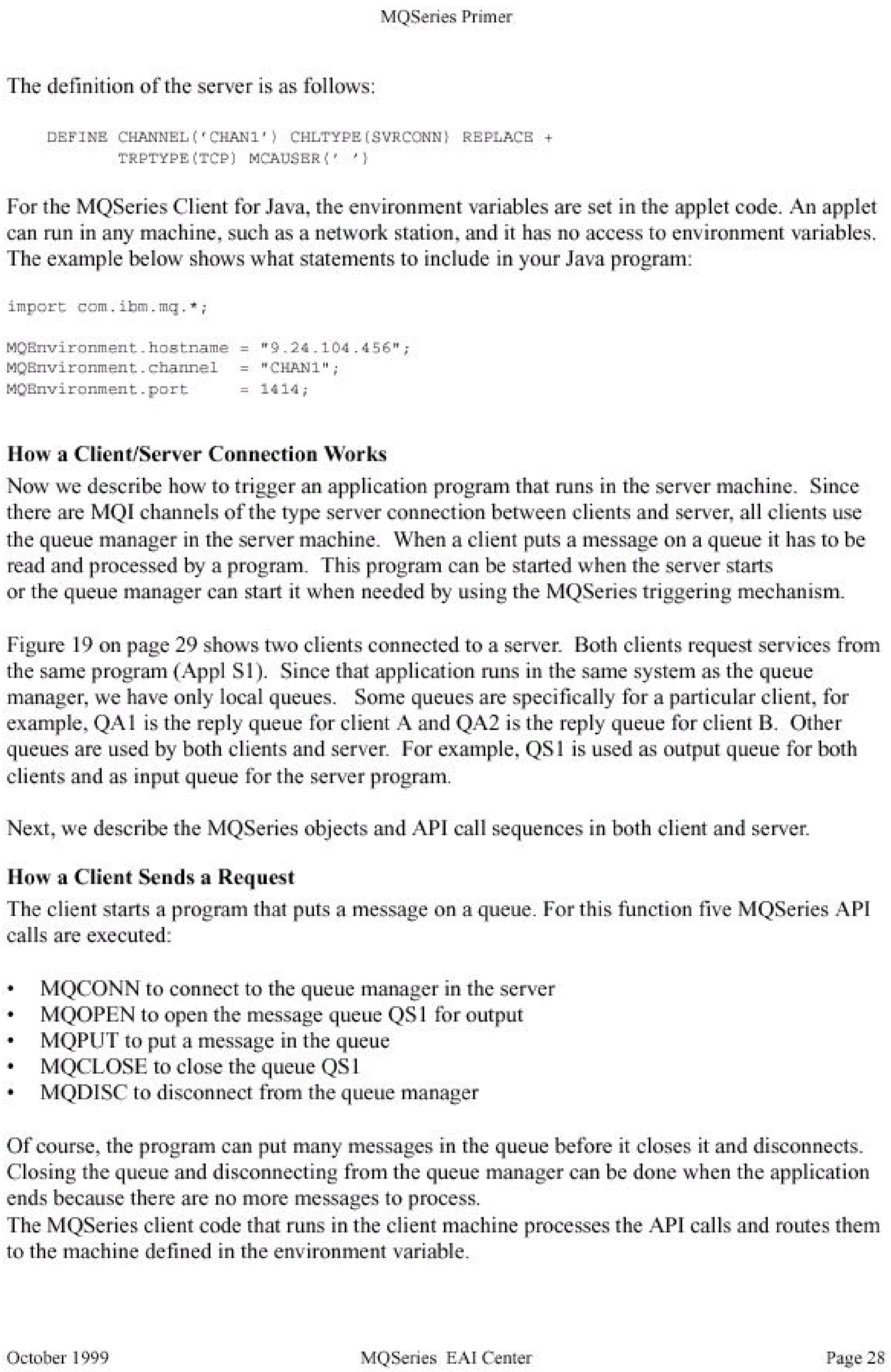
You have to know what transmission protocol is used (for example, TCP/IP), the port the listener listens to (1414 is the default), and the address of the systems to which you want to connect. For an address you can specify an LU name, a host name or machine name, or a TCP/IP address.

The client connection channel is defined as an environment variable, such as:

set MQSERVER=CHAN1/TCP/9.24.104.206(1414)

where:

- MQSERVER is the name of the environment variable.
- CHAN1 is the name of the channel to be used for communication between client and server. This channel is defined in the server. MQSeries will automatically create it should it not exist.
- TCP denotes that TCP/IP is to be used to connect to the machine with the address following the parameter.
- 1414 is the default port number for MQSeries. You may omit this parameter if the listener on the server side uses this default, too.



The definition of the server is as follows:

```
    DEFINE CHANNEL('CHAN1') CHLTYPE(SVRCONN) REPLACE +
           TRPTYPE(TCP) MCAUSER(' ')
```

For the MQSeries Client for Java, the environment variables are set in the applet code. An applet can run in any machine, such as a network station, and it has no access to environment variables. The example below shows what statements to include in your Java program:

```
import com.ibm.mq.*;

MQEnvironment.hostname = "9.24.104.456";
MQEnvironment.channel  = "CHAN1";
MQEnvironment.port     = 1414;
```

How a Client/Server Connection Works

Now we describe how to trigger an application program that runs in the server machine. Since there are MQI channels of the type server connection between clients and server, all clients use the queue manager in the server machine. When a client puts a message on a queue it has to be read and processed by a program. This program can be started when the server starts or the queue manager can start it when needed by using the MQSeries triggering mechanism.

Figure 19 on page 29 shows two clients connected to a server. Both clients request services from the same program (Appl S1). Since that application runs in the same system as the queue manager, we have only local queues. Some queues are specifically for a particular client, for example, QA1 is the reply queue for client A and QA2 is the reply queue for client B. Other queues are used by both clients and server. For example, QS1 is used as output queue for both clients and as input queue for the server program.

Next, we describe the MQSeries objects and API call sequences in both client and server.

How a Client Sends a Request

The client starts a program that puts a message on a queue. For this function five MQSeries API calls are executed:

- MQCONN to connect to the queue manager in the server
- MQOPEN to open the message queue QS1 for output
- MQPUT to put a message in the queue
- MQCLOSE to close the queue QS1
- MQDISC to disconnect from the queue manager

Of course, the program can put many messages in the queue before it closes it and disconnects. Closing the queue and disconnecting from the queue manager can be done when the application ends because there are no more messages to process.
The MQSeries client code that runs in the client machine processes the API calls and routes them to the machine defined in the environment variable.

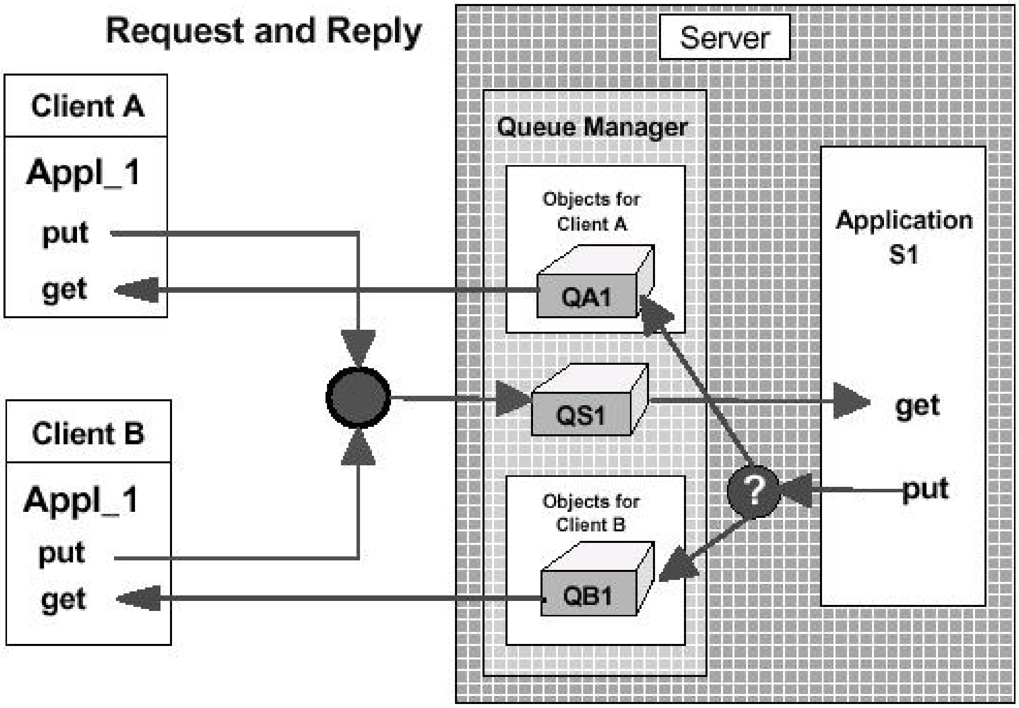


Figure 19. Clients and Server Communicating

How the Server Receives a Request

In the server machine, the following queue manager objects are needed:

- A channel of the type server connection.
- A local queue, QS1, into which the clients put their messages.
- An initiation queue into which the queue manager puts a trigger message when a request for queue QS1 arrives. You can use the default initiation queue.
- A process definition that contains the name of the program to be started when the trigger event occurs (S1).
- One or more queues in which the program puts the reply messages (QA1 and QB1).

In the server machine, two programs have to be started: the listener and the trigger monitor. The listener listens for messages on the channel and puts them on the queue QS1. Since QS1 is triggered, the MQM puts a trigger message on the trigger queue each time a message is put on QS1. When a message is placed on the trigger queue, the trigger monitor starts the program defined in the process.

The server program S1 connects to the queue manager, opens the queue QS1 and issues an MQGET to read the message.

How the Server Sends a Reply

After processing a request the server puts the reply in the reply queue for the client. To do this it has to open the output queue (QA1 or QB1) and issue an MQPUT.

Since several clients use the same server application, it is advisable to give the server a "return address," that is, the names of the queue and the queue manager that will receive the reply message. These fields are in the header of the request message, containing the reply-to-queue manager and reply-to-queue (here, QA1 or QB1). It is the responsibility of the client program to specify these values.

Usually, the server program stays active and waits for more messages, at least for a certain time. For how long can be specified in the wait option of the MQGET API.

How the Client Receives a Reply

The client program knows the name of its input queue, here QA1 or QB1. The application can use two modes of communication:

- *Conversational*
  If the application uses this mode of communication with the server program, it waits for the message to arrive before it continues processing. This means, the reply queue is open and an MQGET with wait option has been issued.

  The client application must be able to deal with two possibilities:

  - The message arrives in time.
  - The timer expires and no message is there.

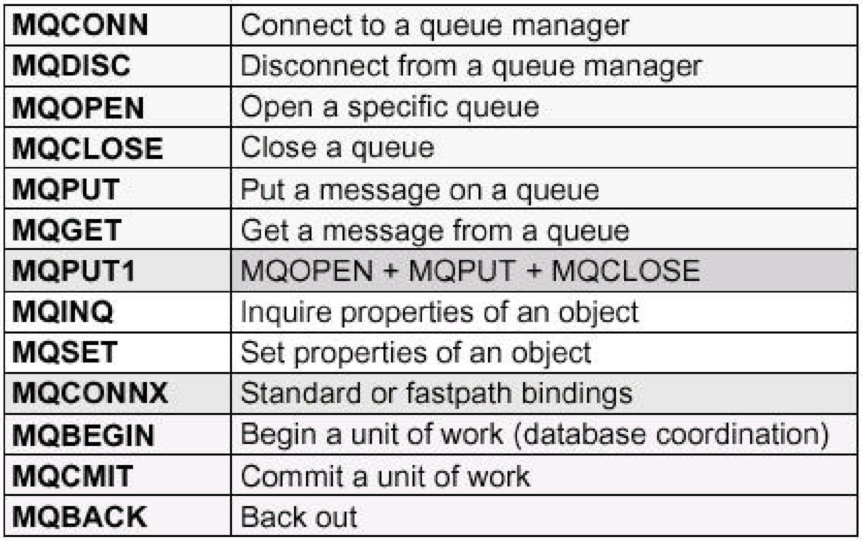
- *True asynchronous*
  When using this mode, the client does not care when the request message arrives. Usually, the user clicks a push button in a menu window to activate a program that checks the reply queue for messages. If a message is present, this or another program can process the reply.

The Message Queuing Interface (MQI)

A program talks directly to its local queue manager. It resides in the same processor or domain (for clients) as the program itself. The program uses the Message Queuing Interface (MQI). The MQI is a set of API calls that request services from the queue manager.

Note: When the connection between a client and its server is broken, no API calls can be executed, since all objects reside in the server.

There are 13 APIs. They are shown in Figure 20 on page 31.



MQCONN	Connect to a queue manager
MQDISC	Disconnect from a queue manager
MQOPEN	Open a specific queue
MQCLOSE	Close a queue
MQPUT	Put a message on a queue
MQGET	Get a message from a queue
MQPUT1	MQOPEN + MQPUT + MQCLOSE
MQINQ	Inquire properties of an object
MQSET	Set properties of an object
MQCONNX	Standard or fastpath bindings
MQBEGIN	Begin a unit of work (database coordination)
MQCMIT	Commit a unit of work
MQBACK	Back out

Figure 20. MQSeries APIs

The most important ones are MQPUT and MQGET. The other calls are used less frequently. Comments regarding several APIs follow:

MQCONN establishes a connection with a queue manager using the standard bindings.

MQCONNX establishes a connection with a queue manager using fastpath bindings. Fastpath puts and gets are faster, but the application must be well behaved, that is, well tested. Application and queue manager run in the same process. When the application crashes it takes the queue manager down with it. This API call is new in MQSeries Version 5.

MQBEGIN begins a unit of work that is coordinated by the queue manager and that may involve external XA-compliant resource managers. This API has been introduced with MQSeries Version 5. It is used to coordinate transactions that use queues (MQPUT and MQGET under syncpoint) and database updates (SQL commands).

MQPUT1 opens a queue, puts a message on it and closes the queue. This is a combination of MQOPEN, MQPUT and MQCLOSE.

MQINQ requests information about the queue manager or one of its objects, such as the number of messages in a queue.

MQSET changes some attributes of an object.

MQCMIT specifies that a syncpoint has been reached. Messages put as part of a unit of work are made available to other applications. Messages retrieved as part of a unit of work are deleted.

MQBACK tells the queue manager to back out all message puts and gets that have occurred since the last syncpoint. Messages put as part of a unit of work are deleted. Messages retrieved as part of a unit of work are reinstated on the queue.

Notes:

- MQDISC implies the commit of a unit of work. Ending the program without disconnecting from the queue manager causes a rollback (MQBACK).
- MQSeries for AS/400 does not use MQBEGIN, MQCMIT or MQBACK. The commit control operation codes of the AS/400 language are used.

A Code Fragment

The code fragment below shows the APIs to put a message on one queue and get the reply from another queue.

Note: The fields CompCode and Reason will contain completion codes for the APIs. You can find them in the Application Programming Reference

Comments:

1 This statement connects the application to the queue manager with the name MYQMGR. If the parameter QMName does not contain a name, then the default queue manager is used. MQ stores the handle of the queue manager in the variable HCon. This handle must be used in all subsequent APIs.

2 To open a queue the queue name must be moved into the object descriptor that will be used for that queue. This statement opens QUEUE1 for output only (open option MQOO_OUTPUT). The handle to the queue and values in the object descriptor are returned. The handle Hobj1 must be specified in the MQPUT.

3 MQPUT places the message assembled in a buffer on a queue. Parameters for MQPUT are:
•The handle of the queue manager (from MQCONN)
•The handle of the queue (from MQOPEN)
•The message descriptor
•A structure containing options for the put (refer to the Application Programming Reference)
•The message length
•The buffer containing the data

4 This statement closes the output queue. Since the queue is predefined no close processing takes place (MQOC_NONE).

5 This statement opens QUEUE2 for input only using the queue-defined defaults. You could also open a queue for browsing, meaning that the message will not be removed.

```
MQHCONN  HCon;                    // Connection handle
MQHOBJ   HObj1;                   // Object handle for queue 1
MQHOBJ   HObj2;                   // Object handle for queue 2
MQLONG   CompCode, Reason;        // Return codes
MQLONG   options;
MQOD     od1 = {MQOD_DEFAULT};   // Object descriptor for queue 1
MQOD     od2 = {MQOD_DEFAULT};   // Object descriptor for queue 2
MQMD     md  = {MQMD_DEFAULT};   // Message descriptor
MQPMO    pmo = {MQPMO_DEFAULT}; // Put message options
MQGMO    gmo = {MQPMO_DEFAULT}; // Get message options
:
//  1  Connect application to a queue manager.
strcpy  (QMName,"MYQMGR");
MQCONN  (QMName, &HCon, &CompCode, &Reason);

//  2  Open a queue for output
strcpy  (od1.ObjectName,"QUEUE1");
MQOPEN  (HCon,&od1, MQOO_OUTPUT, &Hobj1, &CompCode, &Reason);

//  3  Put a message on the queue
MQPUT   (HCon, Hobj1, &md, &pmo, 100, &buffer, &CompCode, &Reason);

//  4  Close the output queue
MQCLOSE (HCon, &Hobj1, MQCO_NONE, &CompCode, &Reason);

//  5  Open input queue
options = MQOO_INPUT_AS_Q_DEF;
strcpy  (od2.ObjectName, "QUEUE2");
MQOPEN  (HCon, &od2, options, &Hobj2, &CompCode, &Reason);

//  6  Get message
gmo.Options = MQGMO_NO_WAIT;
buflen  = sizeof(buffer - 1);
memcpy (md.MsgId, MQMI_NONE, sizeof(md.MsgId);
memset (md.CorrelId, 0x00, sizeof(MQBYTE24));
MQGET (HCon, Hobj2, &md, &gmo, buflen, buffer, 100, &CompCode, &Reason);

//  7  Close the input queue
options = 0;
MQCLOSE (HCon, &Hobj2,options, &CompCode, &Reason);

//  8  Disconnect from queue manager
MQDISC  (HCon, &CompCode, &Reason);
```

Figure 21. A Code Fragment

6 For the get, the nowait option is used. The MQGET needs the length of the buffer as an input parameter. Since there is no message ID or correlation ID specified, the first message from the queue is read. You may specify a wait interval (in milliseconds) here. You can check the return code to find out if the time has expired and no message arrived.

7 This statement closes the input queue.

8 The application disconnects from the queue manager.